Catalogo dei CORSI
2015



/ Business Management

/ *Information & Communication Technology*

/ Percorsi per le certificazioni



Catalogo dei CORSI 2015 /

/ Business Management

/ Information & Communication Technology

/ Percorsi per le certificazioni

UNI EN ISO 9001:2008



Catalogo 2015

Information & Communication Technology

Reiss Romoli s.r.l.
Tel. 0862 452401 - Fax 0862 028308
corsi@ssgrr.com

sede legale - Via Eusanio Stella, 17 - 67100 L'Aquila
sede operativa – Via E. Berlinguer - Z.I. di Pile - 67010 L'Aquila
P.Iva 01800170662

Indice

Reiss Romoli s.r.l. è nata nel 2010 da un gruppo di professionisti con l'obiettivo di concorrere, con il loro lavoro, al successo delle aziende clienti.
Il nome della azienda è un omaggio alla realtà dalla quale proveniamo, la Scuola Superiore Guglielmo Reiss Romoli, ma è anche il segno della nostra determinazione a mantenere viva una tradizione che sa guardare al futuro.

Un impegno che ogni giorno rinnova in noi

la passione della conoscenza



Reiss Romoli è

- ***Testing Person Vue***



- ***IPV6 Training Provider***

Gli esami di certificazione si possono sostenere all'Aquila in Reiss Romoli e nelle sedi di svolgimento dei corsi.

valorizza il capitale umano e migliora le opportunità di business

Formazione

Seminari
Progetti ad hoc
Percorsi di preparazione alle certificazioni di prodotto
Alta formazione post laurea
Eventi

Consulenza

Organizzazione aziendale
Fondi interprofessionali
Assessment tecnologico
Progettazione e reingegnerizzazione di sistemi
Installazione configurazione e assistenza tecnica

METODOLOGIE E STRUMENTI

per una formazione che punta al massimo della qualità

I clienti lo sanno, quando progettiamo i nostri corsi, per tenere alto il valore dell'azione didattica e minimizzarne i costi proponiamo sempre il giusto mix delle diverse modalità.

In aula, dal cliente o in strutture da noi certificate, docenti esperti trasmettono competenze e non solo. Nei nostri corsi c'è sempre innovazione, creatività, realizzazione professionale e personale.

eLearning + aula con le nostre soluzioni "blended" alterniamo lezioni in presenza e a distanza, o integriamo, in aula, metodologie di eLearning con strumenti didattici di tipo tradizionale.

Con il ***Coaching on-line***, nei progetti formativi che prevedono periodi di studio assistito, i nostri esperti interagiscono on line con i partecipanti che svolgono le attività di completamento della preparazione.

Per alcune attività di formazione prevediamo azioni di ***Mentoring*** e cioè l'assistenza dei nostri esperti per la corretta applicazione sul campo di quanto appreso in aula.

Con gli ***Assessment*** individuiamo le necessita formative; analizziamo le risorse umane per valutare le capacità di ricoprire nuovi ruoli o ruoli particolarmente complessi; monitoriamo il processo di apprendimento per misurare l'efficacia degli interventi formativi.

I laboratori di Reiss Romoli, tra i più ricchi in Italia, ***la documentazione didattica***, sempre in lingua italiana e costantemente aggiornata, sono gli strumenti che contribuiscono al successo del nostro modello didattico.

Guida alla consultazione del catalogo

Il volume presenta i nostri corsi sui temi di *Information & Communication Technology.*

La proposta a Catalogo 2015 è organizzato in 3 volumi:

- ✓ ***Information & Communication Technology***
- ✓ ***Business Management***
- ✓ ***Percorsi per le certificazioni***

Le tematiche di Information & Communication Technology

DBS	Basi Dati e Servizi
IPN	Reti IP
IPS	Servizi IP
ITS	Servizi IT
LAP	Linguaggi ed Architetture software
NET	Reti e Servizi di TLC
OPS	Sistemi Operativi
PRJ	Project Management
SCN	Scenari e contesti
SEC	Sicurezza delle Reti e delle Applicazioni
WIR	Reti e Servizi Wireless

Nel Catalogo, i corsi seguono l’ordine alfabetico degli acronimi che identificano le tematiche.

In ciascuna scheda le tre lettere in alto a destra segnalano la tematica alla quale il corso appartiene e dopo il titolo è proposta una breve descrizione dei contenuti, il programma, la durata. Infine sono presentati gli obiettivi che si raggiungono partecipando al seminario, i destinatari ed i prerequisiti.
Nella scheda sono riportati alcuni *simboli*:

ISCRIZIONE GOLD	**Mai più senza il corso!** Nella sezione **Pricing** troverai le informazioni sui vantaggi, su come richiedere questa iscrizione e su come attivare l'**Opzione Gold**.
base *intermedio* *specialistico*	Ogni corso, accanto alla sigla, presenta il **livello di approfondimento**
BLENDED	Indica un percorso **blended** prevede attività d'aula, prework ed attività di coaching, …
CERTIFICAZIONE	Prepara per una **Certificazione**
LABORATORIO	È prevista una intensa attività di esercitazioni, case studies e **laboratorio**
HUMANITAS LUMSA Università	Il corso è progettato ed erogato con HUMANITAS - Centro Universitario di Psicosociologia e Medicina del Lavoro (con la collaborazione Scientifica della Facoltà di Scienze della Formazione dell'Università ***Lumsa*** e dell'Istituto di Psichiatria e Psicologia dell'Università Cattolica del Sacro Cuore di Roma)

La forza di *Reiss Romoli* è nella sua capacità di rispondere - con progetti ad hoc- alle richieste delle aziende clienti.
Se nei nostri cataloghi non c'è il corso che cercavi *chiamaci* o *inviaci un'email* a: *corsi@ssgrr.com*

Information & Communication Technology
Corsi

Basi Dati e Servizi

Reti IP

Servizi IP

Servizi IT

Linguaggi ed Architetture software

Aspetti Legali, Normativi e di Regolamentazione

Reti e Servizi di TLC

Sistemi Operativi

Project Management

Scenari e Contesti

Sicurezza delle Reti e delle Applicazioni

Reti e Servizi Wireless



Basi di dati relazionali: metodologie di progetto e di analisi dei dati

Il corso illustra il processo di progettazione concettuale e logica delle basi di dati relazionali. In particolare, dopo una panoramica generale sulle basi di dati e sui loro sistemi di gestione (DBMS) nell'ambito dei sistemi informatici, illustra in dettaglio tutti gli aspetti relativi alle fasi della progettazione delle basi di dati relazionali: dalla raccolta e analisi dei requisiti alle fasi di progettazione concettuale e logica, alla normalizzazione dello schema relazionale. Per la fase di progettazione concettuale si fa riferimento al modello Entità-Relazioni (E-R), mentre per la creazione e l'utilizzo delle basi di dati è utilizzato il linguaggio SQL. Sono fornite alcune linee guida relative allo sviluppo di applicazioni che interagiscono con le basi di dati. Il corso si conclude con l'analisi e la risoluzione di alcuni casi di studio. Il primo caso di studio propone la progettazione guidata di una base di dati relazionale con discussione degli aspetti più rilevanti di modellazione, mentre gli altri propongono la progettazione di basi di dati di diversa complessità in modalità interattiva.

Agenda (2 giorni)

Introduzione.

Metodologie e modelli di progetto:

- il modello Entità-Relazione.

Progettazione concettuale:

- criteri di progettazione
- strategie di progetto (top-down, bottom-up, mista)
- costrutti base della progettazione concettuale
- entità e relazioni, attributi, identificatori, generalizzazione, documentazione di schemi
- costrutti avanzati della progettazione concettuale
- identificatori esterni, rappresentazione del tempo.

Progettazione logica relazionale:

- analisi e ristrutturazione degli schemi concettuali
- traduzione nel modello relazionale.

Normalizzazione:

- forma normale di Boyce Codd
- decomposizione in forma normale
- proprietà delle decomposizioni
- decomposizione senza perdita e conservazione delle dipendenze.

Casi di studio:

- progettazione concettuale e logica di una base di dati con discussione degli aspetti più rilevanti di modellazione
- progettazione concettuale e logica di strutture di basi di dati di diversa complessità in modalità interattiva.

Obiettivi

Fornire le competenze per progettare un Data Base Relazionale.
Alla fine del corso i partecipanti saranno in grado di progettare un DB relazionale e sviluppare applicazioni per l'analisi dei dati.

Destinatari

Amministratori di Database, Analisti e progettisti software, personale tecnico di supporto.

Prerequisiti

Conoscenze di base di informatica.

Il linguaggio SQL per utenti

Il linguaggio SQL (Structured Query Language) è di fatto lo standard tra i linguaggi per la gestione di data base relazionali. Viene utilizzato dai vari DBMS relazionali (Oracle, Sysbase, SQL-Server, MySql,...) per la definizione, manipolazione e interrogazione delle basi di dati.

Agenda (2 giorni)





Introduzione al linguaggio SQL.

Clausole per estrarre i dati.

Definizione di tabelle e Operazioni di Join.

Inserimento, aggiornamento e cancellazione dei dati.

Transazioni.

Logica sui database relazionali, integrità referenziale.

Select – from-where-group by – order by.

Count –sum- avg e simili.

Operazioni di join, union (No create table, alter, drop).

Comandi per la conversione dei dati (to_data, to_number, to_integer).

Approfondimento su comandi come WITH, coalesce, string, Wbvardef (utilizzo il tool Work Bench) e simili per creare query strutturate e subquery.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare SQL per creare, manipolare e interrogare tabelle per un'analisi strutturata dei dati.

Destinatari

Personale tecnico usa e gestisce data base relazionali.

Prerequisiti

Conoscenze di base di informatica.

Il linguaggio SQL: Base

Il linguaggio SQL (Structured Query Language) è di fatto lo standard tra i linguaggi per la gestione di data base relazionali. Viene utilizzato dai vari DBMS relazionali (Oracle, Sysbase, SQL-Server, MySql,...) per la definizione, manipolazione e interrogazione delle basi di dati.
Il corso, dopo una breve introduzione, illustra le caratteristiche e le logiche del linguaggio nelle sue tre componenti DDL (Data Definition Language), DML (Data Manipolation Language) e in particolare Query Languange. Sono analizzati i comandi per interrogare tabelle in relazione tra di loro utilizzando le clausole.
È previsto un ampio spazio a sessioni di esercitazione con ambiente di riferimento Oracle.

Agenda (3 giorni)





Introduzione al linguaggio SQL.

Clausole per estrarre i dati:

- SELECT
- FROM
- WHERE
- ORDER BY
- GROUP BY
- HAVING.

Operazioni di Join.

Definizione di tabelle.

Definizione di vincoli sulle colonne:

- vincolo Primary Key
- vincolo Foreign Key
- vincolo Not Null
- vincolo Unique
- vincolo Check.

Inserimento, aggiornamento e cancellazione dei dati.

Transazioni.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare SQL per creare, manipolare e interrogare tabelle per un'analisi strutturata dei dati.

Destinatari

Database Administrators, Analisti e progettisti software, programmatori, personale tecnico di supporto.

Prerequisiti

Conoscenze di base di informatica.



Il linguaggio SQL: Avanzato

Poiché il linguaggio SQL (Structured Query Language) è ormai, di fatto, lo standard tra i linguaggi per la gestione di data base relazionali esso viene utilizzato dai vari DBMS relazionali (Oracle, Sysbase, SQL-Server, MySql,…) per la definizione, la manipolazione e l'interrogazione delle basi di dati.
Il corso illustra aspetti avanzati del linguaggio SQL quali: la definizione di subquery, l'utilizzo di funzioni particolari quali CASE, DECODE e NVL. Tra gli oggetti che si possono creare in un database sono presentati gli indici, le viste, le viste materializzate, le sequence. È anche previsto un ampio spazio dedicato a sessioni di esercitazione in ambiente di riferimento Oracle.

Agenda (2 giorni)



Introduzione.

Utilizzo delle funzioni in SQL:

- Stringhe
- Numeri
- Date
- DECODE
- NVL
- CASE
- NULLIF.

Subquery.

Subquery correlate.

Creazione ed esempi di utilizzo dei seguenti oggetti:

- Indici
- Viste
- Viste Materializzate
- Sequence
- Tabelle external.

Gestione degli Utenti:

- creazione utenti
- creazione e gestione dei ruoli
- concessione e revoca dei privilegi.

Introduzione all'architettura di Oracle

Introduzione all'ottimizzazione delle istruzioni SQL.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare costrutti avanzati del linguaggio SQL e creare oggetti nel database.

Destinatari

Database Administrators, Analisti e progettisti software, programmatori, personale tecnico di supporto.

Prerequisiti

Conoscenze di base del linguaggio SQL.



Database in ambiente Oracle: PL/SQL

PL/SQL è un linguaggio di 4^ generazione nato come estensione di SQL standard e consente di intergrare un linguaggio procedurale all'SQL.
Il corso fornisce le conoscenze avanzate per realizzare applicazioni, stored procedure, trigger, package nell'ambito di progetti di basi di dati relazionali in ambiente Oracle. Dopo una breve introduzione sul linguaggio e l'ambiente di riferimento, vengono illustrate in dettaglio le caratteristiche del linguaggio e tutti gli aspetti relativi all'interazione.

Agenda (3 giorni)



Introduzione a PL/SQL (SQL, SQL*Plus, PL/SQL).

Dichiarazioni e blocchi (Tipi di dati, utilizzo della struttura a blocchi).

Espressioni PL/SQL:
- operatori, espressioni e conversioni
- costruzione di espressioni con gli operatori PL/SQL
- utilizzo degli operatori di confronto con stringhe e con date.

Utilizzo di funzioni, condizioni e cicli:
- le funzioni PL/SQL
- l'istruzione NULL; Utilizzo degli statement PL/SQL
- implementare cicli
- utilizzo della ricorsione
- funzioni built-in di Oracle
- confronto tra funzioni SQL e PL/SQL; Utilizzo delle funzioni di conversione.

Procedure, Pacchetti, Errori ed Eccezioni:
- utilizzo di procedure
- i meccanismi di sicurezza in fase di invocazione
- utilizzo di package
- gestione di errori ed eccezioni.

Gestione dei cursori.

Le Collezioni:
- utilizzo di tabelle PL/SQL Index-by
- le tabelle nested
- gli array a dimensione variabile
- vantaggi del bulk-binding
- gestione delle eccezioni nelle collezioni.

Trigger su database.

Utilizzo di oggetti per la programmazione Object-Oriented:
- implementazione degli oggetti in Oracle
- istanziare ed utilizzare gli oggetti
- il parametro SELF
- tabelle di oggetti.

Obiettivi
Al termine del corso i partecipanti saranno in grado di scrivere procedure e funzioni in ambiente Oracle.

Destinatari
Database Administrators, Analisti e progettisti software, programmatori, personale tecnico di supporto.

Prerequisiti
Conoscenza del linguaggio SQL.

Introduzione alla Business Intelligence

La Business Intelligence studia ed analizza le informazioni strategiche in ambito aziendale. I dati operativi utili al supporto dei processi di decisione sono solitamente raccolti in grandi basi di dati denominate Data Warehouse. Il corso introduce le problematiche di progettazione e interrogazione dei Data Warehouse. Descrive le principali tecniche di analisi OLAP comunemente supportate all'interno di un Data Warehouse. Vengono inoltre introdotte le principali tecniche di data mining a supporto del processo di estrazione di conoscenza. L'analisi delle tecniche è incentrata su contesti applicativi reali: la segmentazione dei clienti, il profiling di servizi e clienti, il Customer Relationship Management (CRM), la content curation e la competitive intelligence. Il corso si conclude con lo sviluppo di un caso di studio centrato sulla progettazione e l'implementazione di un Data Warehouse in Microsoft SQL Server 2008 e sull'analisi dei dati mediante lo strumento open source Rapid Miner.

Agenda (2 giorni)



Introduzione alla Business Intelligence:

- dai dati all'informazione
- definizione di Business Intelligence.

Introduzione al Data Warehouse:

- le basi di dati
- obiettivi di un Data Warehouse
- architetture e modelli di Data Warehouse
- progettazione concettuale, logica e fisica di un Data Warehouse
- analisi OLAP dei dati
- SQL esteso
- Roll-up, drill down e pivoting
- Reporting e dashboard.

Introduzione al Data Mining:

- il processo di estrazione di conoscenza (KDD)
- la preparazione dei dati per l'analisi
- classificazione delle tecniche di analisi dei dati
- la classificazione e la regressione
- l'estrazione di regole di associazione
- il clustering.

Applicazioni di Business Intelligence:

- segmentazione dei clienti
- competitive intelligence
- Customer Relationship Management
- Service profiling
- Content curation.

Caso di studio:

- introduzione ai software Microsoft SQL Server 2008 e Rapid Miner
- progettazione di un Data Warehouse e sua implementazione con Microsoft SQL Server 2008
- analisi dei dati mediante lo strumento open source Rapid Miner.

Obiettivi

Al termine del corso i partecipanti saranno in grado di comprendere le metodologie di progettazione di una base di dati, le tecniche di estrazione ed analisi dei dati e le possibili applicazioni commerciali.

Destinatari

Professional interessati alla manipolazione, gestione e archiviazione dati, responsabili e progettisti IT, analisti e programmatori.

Prerequisiti

Conoscenza dei fondamenti delle basi di dati relazionali.

Strumenti per la Business Intelligence

I sistemi informativi finalizzati alla Business Intelligence si servono solitamente, per la raccolta e la gestione dei dati operativi, di grandi basi di dati denominate Data Warehouse. Impiegano, inoltre, tecniche di analisi dei dati tradizionali, quali le analisi OLAP, ed avanzate, quali le tecniche di Data Mining.
Il corso è finalizzato ad analizzare i principali strumenti a supporto della Business Intelligence. Vengono illustrate le tecniche e le tecnologie a supporto della progettazione dei Data Warehouse, dalla Dimension Fact Table, alla generazione di viste materializzate. Vengono affrontate le principali problematiche relative al processo ETL e le più comuni tecniche di analisi e interrogazione dei Data Warehouse aziendali. Viene inoltre affrontato il tema della presentazione dei dati e della reportistica attraverso interfacce grafiche ad hoc. Il corso, infine, introduce le principali tecniche di Data Mining a supporto di analisi complesse e le loro principali applicazioni. Alle lezioni teoriche si alterna lo studio e la realizzazione, a cura dei partecipanti, di casi di studio mediante i software Microsoft SQL Server 2008 per la gestione dei Data Warehouse e Weka per l'applicazione di tecniche di Data Mining.

Agenda (2 giorni)



Progettazione di un Data Warehouse aziendale:

- descrizione del processo di funzionamento di un Data Warehouse
- analisi dei requisiti
- progettazione concettuale mediante Dimensional Fact Table
- gestione del tempo
- progettazione logica e viste materializzate
- progettazione fisica
- operatori di aggregazione
- il processo ETL
- analisi di un caso di studio e implementazione con Microsoft SQL Server 2008.

Analisi tradizionale:

- HyperCube e analisi OLAP
- SQL esteso
- analisi di un caso di studio e implementazione con Microsoft SQL Server 2008.

Dashboard e reportistica:

- strumenti di reportistica
- interfacce grafiche a supporto della Business Intelligence
- information visualization.

Analisi complesse mediante tecniche di Data Mining:

- strumenti per la preparazione e l'integrazione dei dati
- algoritmi di classificazione e regressione
- algoritmi per l'estrazione di itemset frequenti
- algoritmi di clustering partizionali, gerarchici e density-based
- validazione dei risultati
- analisi di un caso di studio e implementazione con lo strumento opensource Weka.

Obiettivi

Alla fine del corso i partecipanti saranno in grado di affrontare i processi aziendali finalizzati al supporto alle decisioni mediante l'uso di strumenti quali i Data Warehouse e le tecniche di analisi dei dati.

Destinatari

Professional interessati alla manipolazione, gestione e archiviazione dati, responsabili e progettisti IT, analisti e programmatori.

Prerequisiti

Conoscenze dei concetti di base di dati relazionali e Data Warehouse.

Data Mining

Le tecniche di Data Mining offrono oggi un supporto sempre più rilevante alle decisioni aziendali attraverso l'analisi dei dati su larga scala. Le metodologie di analisi e gli algoritmi proposti trovano applicazione in svariati ambiti sia commerciali, come il marketing e la competitive intelligence, sia scientifici, come l'analisi di dati biologici e clinici per lo studio di malattie genetiche e la validazione di terapie mediche.
Il corso presenta il processo di analisi ed elaborazione dei dati al fine di estrapolare informazioni utili per il supporto alle decisioni aziendali. Verranno presentate le principali tecniche di analisi dei dati, quali la classificazione, l'estrazione di associazioni, il clustering e le loro principali applicazioni in ambito aziendale. Lezioni teoriche si alterneranno allo sviluppo di casi di studio, la cui progettazione sarà a cura dei partecipanti. I casi di studio prevedono l'utilizzo del software open source Rapid Miner e saranno mirati all'applicazione delle tecniche apprese, all'analisi critica e alla validazione dei risultati.

Agenda (3 giorni)



Introduzione al Data Mining: fondamenti ed applicazioni:

- classificazione delle tecniche di data mining
- analisi dei contesti applicativi.

Preparazione dei dati per l'analisi:

- integrazione e filtraggio dei dati
- aggregazione, discretizzazione e campionamento dei dati
- feature selection
- misure di distanza.

Tecniche di analisi dei dati.

Classificazione:

- alberi di decisione
- classificazione basata su regole
- classificazione Bayesiana
- tecniche di validazione.

Estrazione di regole di associazione:

- principali algoritmi
- indici di qualità.

Clustering:

- principali algoritmi
- tecniche di validazione.

Strumenti per il Data Mining:

- classificazione dei software
- introduzione al software open source Rapid Miner
- uso di Rapid Miner per la preparazione, classificazione, clustering e visualizzazione dei dati.

Casi di studio:

- creazione di una base di dati e preparazione dei dati da analizzare mediante Rapid Miner
- classificazione di dati mediante Rapid Miner
- estrazione di regole di associazione mediante Rapid Miner.

Obiettivi

Al termine del corso i partecipanti saranno in grado di implementare ed utilizzare le principali tecniche di estrazione ed analisi dei dati contenuti in una base di dati relazionale.

Destinatari

Professional interessati alla manipolazione, gestione e archiviazione dati, responsabili e progettisti IT, analisti e programmatori.

Prerequisiti

Nessuno.



Data Mining per il supporto alle decisioni aziendali

L'analisi dei dati è una problematica di fondamentale importanza all'interno del contesto aziendale. Se le basi di dati e i relativi sistemi di gestione consentono oggi di gestire collezioni di dati di dimensioni sempre maggiori, la scelta delle tecniche di analisi più opportune per la generazione di conoscenza fruibile a partire dai dati stessi rappresenta il passo più complesso e decisivo per il supporto alle decisioni aziendali.
Il corso analizza lo sviluppo del processo di estrazione di conoscenza basato su tecniche di Data Mining (KDD) applicato a contesti reali di analisi in ambito aziendale. Viene illustrata l'applicazione delle principali tecniche di analisi dei dati e validazione dei risultati finalizzate alle risoluzione di problematiche aziendali quali la personalizzazione dei servizi, la segmentazione dei clienti, il cross-marketing e i recommendation system. Il corso si conclude con un caso di studio, interamente progettato dai partecipanti, che prevede l'utilizzo di tecniche e algoritmi di Data Mining e del software open source Rapid Miner.

Agenda (2 giorni)



Il processo di estrazione di conoscenza:
- preparazione dei dati all'analisi
- classificazione delle tecniche di analisi
- validazione dei risultati e reporting.

La personalizzazione dei servizi:
- analisi del contesto applicativo
- estrazione di regole di associazione per la personalizzazione dell'offerta
- profiling di utenti e servizi
- validazione dei risultati ottenuti.

La segmentazione della clientela:
- analisi del contesto applicativo
- applicazione di tecniche di clustering per la segmentazione dei clienti
- misure di qualità.

I recommendation system:
- analisi del contesto applicativo
- applicazione di tecniche di classificazione per la raccomandazione di prodotti o servizi
- validazione dei risultati
- applicazione al cross-marketing.

Strumenti per il Data Mining:
- categorie di software
- introduzione al software open source Rapid Miner
- uso di Rapid Miner per l'analisi dei dati.

Caso di studio:
- definizione di un contesto applicativo di interesse
- creazione di una base di dati da analizzare
- analisi dei dati mediante Rapid Miner
- validazione dell'analisi.

Obiettivi

Al termine del corso i partecipanti saranno in grado di applicare le principali tecniche di estrazione ed analisi dei dati a problematiche aziendali reali.

Destinatari

Professional interessati alla manipolazione, gestione e archiviazione dati, responsabili e progettisti IT, analisti e programmatori.

Prerequisiti

Conoscenza di base delle principali tecniche di analisi di dati.



Data Warehouse: analisi dei dati a supporto delle decisioni aziendali

Un Data Warehouse permette di raccogliere rilevanti quantità di dati, estratti da basi di dati di tipo eterogeneo su cui operano le diverse applicazioni di un'azienda, e di renderli disponibili, interpretabili e utilizzabili a supporto delle decisioni strategiche aziendali. Nel corso i Data Warehouse sono descritti sia dal punto di vista architetturale che tecnologico. Dopo una dettagliata presentazione delle diverse architetture funzionali adottabili, viene analizzato criticamente l'intero processo che porta all'implementazione di un sistema di Data Warehouse. Vengono descritte le fasi che portano dalla progettazione dello schema concettuale mediante il Dimensional Fact Model (DFM) alla progettazione dello schema logico (in ambito relazionale) e fisico. Vengono poi presentate e discusse le fasi relative al processo di alimentazione di un Data Warehouse. Infine, per quanto riguarda l'interrogazione, vengono trattate sia le tecniche di analisi OLAP dei dati che l'estensione del linguaggio SQL. Il corso si conclude con due casi di studio: il primo propone la progettazione guidata di un Data Warehouse con discussione degli aspetti più rilevanti di modellazione, il secondo propone un Data Warehouse interamente progettato dai partecipanti ed implementato utilizzando Microsoft SQL Server.

Agenda (5 giorni)



Introduzione al Data Warehouse:

- scenario, motivazioni, definizioni e concetti di base
- architetture per Data Warehouse; struttura ed elaborazione dei dati.

Modellazione concettuale di un Data Warehouse:

- analisi dei requisiti
- il Dimensional Fact Model (DFM): concetti di base ed avanzati.

Progettazione logica:

- modello relazionale (ROLAP)
- schemi a stella, schema snowflake, archi multipli, dimensioni degeneri
- viste materializzate; scelta delle viste.

Progettazione fisica e analisi dell'allocazione dei dati.

Progettazione dell'alimentazione:

- alimentazione dello schema riconciliato
- pulizia dei dati
- alimentazione delle tabelle dei fatti e delle viste materializzate.

Analisi OLAP.

Estensioni del linguaggio SQL:

- funzioni OLAP in SQL
- finestre di calcolo; calcolo di totali cumulativi
- operatore group by e finestre di calcolo; estensioni della clausola group by
- funzioni di ranking.

Caso di studio 1:

- progettazione (concettuale e logica) guidata di un Data Warehouse con discussione degli aspetti più rilevanti di modellazione.

Caso di studio 2:

- progettazione (concettuale e logica) di un Data Warehouse da parte dei partecipanti ed implementato utilizzando Microsoft SQL Server.

Obiettivi

Alla fine del corso i partecipanti sono in grado di progettare un Data Whareouse ed utilizzarlo per varie finalità e analizzare le possibili applicazioni.

Destinatari

Responsabili e progettisti IT, Database Administrators, Analisti e programmatori, progettisti software.

Prerequisiti

Conoscenze dei concetti di basi di dati relazionali.



Sviluppo di procedure ETL in Datastage

Il corso descrive le caratteristiche di IBM InfoSphere DataStage e insegna come costruire e gestire job DataStage Extract, Transform and Load (ETL). Sono illustrate e fornite le nozioni per costruire job server e paralleli in DataStage, in grado di leggere e scrivere dati da e su una varietà di archivi, inclusi i file sequenziali, dataset e tabelle relazionali. A completamento della trattazione teorica, sono previste numerose esercitazioni.

Agenda (4 giorni)



Introduzione a Datastage.

Utilizzo degli strumenti di Datastage:

- Console di amministrazione
- Designer
- Director
- Amministratore.

Recupero e scrittura di dati relazionali utilizzando connettori su database e flat file.

Job server (Aggregator, Merge, Sort, Transformer).

Job parallel (Aggregator, Transformer, Funnel, Join, LookUp, Sort, Remove Duplicates).

Definizione di Sequence.

Defінzione di Routines.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze teoriche e pratiche su come definire job server e paralleli di Datastage.

Destinatari

Analisti e sviluppatori ETL programmatori, amministratori di progetto.

Prerequisiti

Conoscenza di SQL.

Ethernet: dalle Reti Locali alle Reti Metropolitane

Il protocollo Ethernet è da anni lo standard di riferimento per la realizzazione di reti locali. Grazie alla scalabilità, che ha portato ad un incremento delle prestazioni di diversi ordini di grandezza, nonché alla semplicità ed economicità di implementazione, Ethernet è uscito dall'ambito delle reti locali per essere utilizzato diffusamente anche nelle reti metropolitane e geografiche.
Il corso fornisce un'ampia panoramica sulle caratteristiche di una rete locale e sui protocolli che ne governano il funzionamento. Le tecnologie descritte sono poi contestualizzate nell'ambito della loro applicazione all'architettura di 'Reti di Campus', sia di livello 2 che multilayer, ed alle applicazioni in ambito metropolitano.

Agenda (3 giorni)

Ethernet e le LAN (Local Area Network):

- i protocolli per le LAN e lo standard 802.3
- topologie a bus condiviso e a stella
- la trama e gli indirizzi Ethernet
- il livello MAC e la contesa del mezzo
- Switched Ethernet.

Evoluzione di Ethernet:

- Fast Ethernet e Gigabit Ethernet
- nuovi standard a 10, 40 e 100 Gigabit/s
- Virtual LAN
- configurazione di apparati per reti locali:
- configurazione delle interface e configurazione di VLAN.

Lo spanning Tree Protocol:

- il protocollo STP
- il protocollo Rapid Spanning Tree e la variante Cisco PV-RSTP
- il Multiple Spanning Tree Protocol (MST).

Multilayer Switching:

- funzionalità di InterVLAN routing
- architettura dei multilayer switch
- cenni sui protocolli di Next Hop redundancy (HSRP, VRRP, GLBP).

Architetture di reti di Campus:

- caratteristiche generali
- il modello Multi-tier e le sue varianti.

Ethernet nelle reti metropolitane:

- architettura di una rete Metro Ethernet
- alternative trasmissive
- Ethernet su SDH e Ethernet su WDM
- interconnessione con Switch Layer 2 e 3
- utilizzo delle VLAN nelle Metro Ethernet, Stacked VLAN.

Esempi di utilizzo delle reti Metro Ethernet:

- accesso alle reti IP, backhauling per xDSL, IP-TV,accesso FTTH.

Obiettivi

Acquisire le conoscenze sui meccanismi di funzionamento delle LAN.
Essere in grado di identificare le categorie di apparati più adatti alle diverse tipologie di rete.
Conoscere l'architettura delle reti metropolitane basate sulla tecnologia Ethernet.

Destinatari

Il corso è rivolto a chi abbia l'esigenza di acquisire una buona conoscenza di base sulle reti LAN utilizzate sia in ambito locale che metropolitano.

Prerequisiti

Conoscenze di base delle reti di TLC e del protocollo IP.

Le Reti Metro Carrier Ethernet

Il corso fornisce un'ampia panoramica sui principi e le soluzioni adottate nelle moderne reti di accesso basate sulla tecnologia Ethernet applicata in ambito metropolitano.
Dopo brevi richiami sulla tecnologia Ethernet e la sua evoluzione, verranno descritti i servizi definiti dal Metro Ethernet Forum, i parametri per valutare le prestazioni, gli standard principali, le architetture di rete e i relativi apparati. Saranno illustrate le modalità di interazione con le reti IP dei Service Provider e i servizi erogabili. Una parte significativa del corso è dedicata alle soluzioni adottate sul campo per evitare i problemi di scalabilità tipici dello standard Ethernet, come ad esempio l'utilizzo dell'incapsulamento MAC-in-MAC e l'utilizzo dello standard MPLS. Il corso descrive le principali raccomandazioni fornite dal 'Metro Ethernet Forum' (MEF) per accelerare l'adozione a livello globale delle reti e dei servizi 'Carrier-class Ethernet'. Saranno infine presentati alcuni case study in cui si descrivono possibili architetture di reti Carrier Ethernet ed i servizi che con esse è possibile offrire.

Agenda (2 giorni)

Richiami su Ethernet, VLAN e Multilayer Switching.

Estensione di Ethernet dall'ambito locale all'ambito metropolitano:
- architettura di reti Metro Ethernet
- tecnologie per il primo miglio (IEEE802.3ah e IEEE802.3-2008)
- Ethernet Nativo.

Tecnologie per la Carrier Ethernet:
- modello QinQ e Provider Bridge (standard IEEE 802.1ad)
- modello MAC-in-MAC e Provider Backbone Bridge (standard IEEE 802.1ah)
- Ethernet su MPLS e Generalised MPLS.

Aspetti di QoS e di scalabilità.

Aspetti di OAM e SLA performance:
- funzionalità del Demarcation device
- Service Layer OAM (UNI to UNI) (IEEE 802.1ag / ITU-T Y.1731)
- Connectivity Layer OAM e Access Link OAM.

Il Metro Ethernet Forum (MEF) e le sue principali specifiche:
- architettura di riferimento
- interfacce UNI e E-NNI
- definizione dei servizi di L2VPN su reti Metro/Carrier Ethernet
- accordi di implementazione
- Test Suite e conformità (Es. Certificazione MEF 9&14).

Case Study di rete Metro Carrier Ethernet:
- servizi commerciali (per Clienti Business, Residenziali e OLO)
- servizi End to End, End to POP e POP to POP
- architettura di rete e soluzioni tecniche
- applicazioni: Mobile Backhauling, IPTV.

Obiettivi

Al termine del corso i partecipanti avranno acquisito conoscenze su:
- i modelli architetturali e le tecnologie per il trasporto di Ethernet in reti ISP
- i servizi definiti in ambito MEF relativi allo sviluppo di Carrier-class Ethernet
- le modalità di gestione e di misura dei parametri di qualità nelle reti Carrier-Ethernet
- le principali raccomandazioni MEF.

Destinatari

Personale, sia tecnico che commerciale con competenze tecnologiche, di ISP o di aziende clienti e quanti interessati a servizi di connettività metropolitana o geografica in ambiente MEF (Metro Ethernet Forum).

Prerequisiti

Conoscenza generale delle reti IP, in particolare del routing IP e dello standard MPLS.

Introduzione alle reti per dati ed al Cisco IOS

Il corso fornisce le conoscenze di base sui protocolli di comunicazione dati, con particolare riferimento all'architettura TCP/IP e ad Internet, ed ai protocolli ed alle tecnologie utilizzate in ambito LAN/Ethernet. Nel corso si introducono anche i meccanismi di switching e di routing, mettendoli in pratica attraverso esercitazioni di laboratorio di livello introduttivo svolte su apparati Cisco. Tali esercitazioni costituiscono anche lo strumento per 'familiarizzare' con il sistema operativo IOS di Cisco.
Il corso è parte del programma per acquisire la preparazione necessaria per sostenere l'esame di certificazione Cisco 200-120 "Cisco Certified Network Associate (CCNA)".

Agenda (5 giorni)





Principi di comunicazione dati:
- architetture e protocolli di comunicazione
- reti per dati a circuito e a pacchetto
- principi di comunicazione dati e modelli stratificati
- il modello di riferimento ISO/OSI
- servizi Connectionless e Connection-Oriented
- architetture di rete per dati WAN.

Architettura TCP/IP:
- internetworking e architettura TCP/IP
- internet Protocol (IP): funzionalità di IP ed indirizzamento
- conversione degli indirizzi IP in indirizzi fisici (ARP)
- esercitazione teorica: costruzione di un piano di indirizzamento IP con VLSM
- Internet Control Message Protocol (ICMP)
- protocolli di livello trasporto: UDP e TCP
- il Dynamic Host Configuration Protocol (DHCP)
- indirizzamento privato e Network Address Translation (NAT)
- i principali Applicativi su reti IP.

Architetture di rete locale (LAN):
- reti LAN: mezzi trasmissivi, topologie e protocolli di accesso
- il modello IEEE 802: livello fisico, MAC ed LL
- il protocollo IEEE 802.3
- evoluzione di Ethernet: da 10 Mbit/s a 100Gbit/s
- cenni sul protocollo dello Spanning Tree e Rapid Spanning Tree
- introduzione su Bridging e Switching
- domini di collisione; learning e filtraggio delle trame
- tabelle degli indirizzi MAC (CAM)
- Virtual LAN e trunking.

Il Cisco IOS e la Command line interface (CLI):
- configurazioni di base degli switch Cisco
- il processo di bootstrap ed il registro di configurazione
- gestione delle configurazioni e delle immagini di IOS
- introduzione al Cisco.

Introduzione al routing IP:
- funzionalità di routing e forwarding; Tabelle di routing; Routing statico e dinamico
- la configurazione di base di un router
- protocolli di routing Distance Vector e Link State
- distanza amministrativa, metrica, convergenza
- il protocollo RIP ed il RIPv2 e cenni sul protocollo OSPF.

Laboratori ed Esercitazioni:
- definizione di un piano di indirizzamento IP
- configurazioni di base di uno switch Cisco
- configurazioni di base di un router Cisco e di routing statico
- configurazione di RIP ed OSPF in singola area.

Introduzione alle reti per dati ed al Cisco IOS

Obiettivi

Comprendere la struttura ed i meccanismi base di funzionamento dei protocolli dell'architettura TCP/IP.
Acquisire conoscenze di base sulle tecnologie Ethernet.
Apprendere i principi di base sul funzionamento di switch e router.
Familiarizzare con il Cisco (IOS).

Destinatari

Chi sta iniziando un percorso di formazione sulle reti IP.
Tecnici di rete ed operatori di help desk che operino nel settore del networking, o ad altre figure professionali che abbiano bisogno di acquisire competenze introduttive sulla configurazione e la gestione di router e switch Cisco.

Prerequisiti

Nessuno.

Internet e il protocollo IP per non tecnici

La diffusione nell'ultimo decennio del modello "*all IP*", cioè la tendenza ad integrare tutti i differenti servizi di telecomunicazione (voce, dati, video, etc.) sotto l'unico paradigma del protocollo IP, e soprattutto l'utilizzo di IP nel mondo della telefonia mobile, rendono la conoscenza del funzionamento di Internet e del protocollo IP ormai imprescindibile per chiunque operi nel mondo delle TLC. Il corso descrive le principali caratteristiche ed i meccanismi di funzionamento dei protocolli che sono alla base della suite TCP/IP.

Agenda (2 giorni)

Le reti per dati.

Le architetture protocollari: il modello ISO-OSI.

Le reti LAN e il protocollo Ethernet.

Internet: architettura e servizi.

Introduzione ad Internet e all'architettura TCP/IP.

Il protocollo IPv4.

Il protocollo IPv6.

Principi di routing:

DHCP (Dynamic Host Configuration Protocol)

I protocolli TCP e UDP.

Le principali applicazioni.

Obiettivi

Al termine del corso i partecipanti:

- conosceranno i meccanismi di funzionamento delle reti IP
- conosceranno le modalità di funzionamento dei principali servizi di rete
- avranno acquisito una panoramica sull'evoluzione del protocollo IP e sulle nuove applicazioni
- sapranno svolgere semplici operazioni e configurazioni di troubleshooting su una rete IP.

Destinatari

Il corso è rivolto a tutti coloro che abbiano l'esigenza di aquisire competenze di base sull'architettura Internet e sulla sua evoluzione verso IPv6.

Prerequisiti

Nessuno.

Fondamenti di Internet, IPv4 ed IPv6

La diffusione nell'ultimo decennio del modello "*all IP*", cioè della tendenza ad integrare tutti i differenti servizi di telecomunicazione (voce, dati, video, etc.) sotto l'unico paradigma del protocollo IP, e soprattutto l'utilizzo di IP nel mondo della telefonia mobile, ha accelerato il passaggio da IPv4 ad IPv6. La transizione si completerà nei i prossimi anni e nel frattempo dovremo "convivere" con entrambe le versioni del protocollo IP.
Il corso descrive le principali caratteristiche ed i meccanismi di funzionamento dei protocolli che sono alla base della suite TCP/IP, mettendo in evidenza le differenze tra la versione v4 e quella v6. Segue una descrizione delle principali applicazioni basate su IP. La trattazione teorica è arricchita da esercitazioni "hands on" sulla configurazione di IP, su PC e su apparati di rete Cisco, per riprodurre, in laboratorio, situazioni analoghe a quelle reali in ambienti LAN e WAN.

Agenda (5 giorni)



Richiami sulle LAN e configurazione di apparati per reti locali (SWITCH).

Introduzione ad Internet e all'architettura TCP/IP.

Il protocollo IPv4:

- il pacchetto e gli indirizzi IP
- risoluzione degli indirizzi (Address Resolution Protocol)
- indirizzamento pubblico e privato, NAT e PAT.
- Il protocollo ICMP.

Il protocollo IPv6:

- motivazioni per la migrazione
- principali differenze rispetto ad IPv4
- il protocollo ICMPv6
- stateless address autoconfiguration (SLAAC).

Esercitazione teorica: definizione di un piano di indirizzamento IPv4 ed IPv6.

Laboratorio 1: configurazione di PC con IPv4 ed IPv6, ed analisi di protocollo con Wireshark.

Principi di routing:

- l'instradamento nelle reti IP
- interconnessione di LAN tramite router
- algoritmi e protocolli di routing
- routing intradominio e interdominio, routing multicast
- differenze tra i protocolli di routing per IPv4 e per IPv6
- esempi di configurazione di protocolli di routing.

Introduzione alla configurazione di router CISCO.

DHCP (Dynamic Host Configuration Protocol)

- Il DHCP per IPv4
- Il DHCP per IPv6: statefull DHCPv6 e DHCPv6 lite.

I protocolli TCP e UDP.

Le principali applicazioni:

- DNS (Domain Name System)
- FTP (File Transfer Protocol)
- il protocollo HTTP e il World Wide Web
- i protocolli per l'e-mail.

Laboratorio 2: configurazione di base di router Cisco per routing IPv4 ed IPv6.

I meccanismi di migrazione e convivenza tra IPv4 ed IPv6:

- Dual Stack
- meccanismi di tunnelling automatico: 6to4, 6rd, ISATAP, Teredo
- Tunnel Brocker e TSP
- Dual stack lite e NAT64/DNS64.

Fondamenti di Internet, IPv4 ed IPv6

Obiettivi

Al termine del corso i partecipanti:

- conosceranno i meccanismi di funzionamento delle reti IP
- conosceranno le principali caratteristiche sia di IPv4 che di IPv6
- saranno in grado di definire un piano di indirizzamento IPv4 ed IPv6
- sapranno identificare il metodo di assegnazione degli indirizzi più adatto
- conosceranno le modalità di funzionamento dei principali servizi di rete
- avranno acquisito una panoramica sull'evoluzione del protocollo IP e sulle nuove applicazioni
- sapranno svolgere semplici operazioni e configurazioni di troubleshooting su una rete IP.

Destinatari

Il corso è rivolto a tutti coloro che abbiano l'esigenza di aquisire competenze di base sull'architettura Internet e sulla sua evoluzione verso IPv6.

Prerequisiti

Conoscenza di base delle reti di telecomunicazione.

Networking IP in ambiente Cisco

Il corso offre una panoramica introduttiva sui meccanismi di switching e di routing, descrivendo le principali tecnologie di livello 2 e 3, con riferimento, in particolare, ad apparati Cisco. Fornisce, inoltre, le competenze di base e la conoscenza del sistema operativo Cisco (IOS) necessarie alla configurazione di apparati Cisco in ambiente LAN e WAN. È prevista una rilevante attività di laboratorio *hands on* su apparati Cisco. Sono utilizzati switch Catalyst e router Cisco per riprodurre situazioni analoghe a quelle riscontrabili nella realtà in ambienti di area locale (LAN) e geografica (WAN) di piccole e medie dimensioni.
Il corso è parte del programma per acquisire la preparazione necessaria per sostenere l'esame di certificazione Cisco 200-120 "Cisco Certified Network Associate (CCNA)".

Agenda (5 giorni)





Introduzione al Cisco Internetworking Operating System (IOS):
- Command Line Interface degli Switch Cisco Catalyst e dei Router Cisco
- cenni su SDM (Security Device Manager).

Switching su apparati Cisco:
- *protocollo di Spanning Tree e configurazione di uno Switch Catalyst.*

Estensione di una rete di switch attraverso Virtual LAN:
- *i protocolli di trunking e il VLAN Trunk Protocol (VTP)*

Routing IP:
- route statiche e loro configurazione; routing dinamico e protocolli di routing; protocolli EIGRP e OSPF.

Gestione del traffico con le Access List:
- *Access List standard ed estese per TCP/IP*
- controllo di accessi telnet sui router.

Introduzione alle reti geografiche (WAN): interfacce WAN sui router Cisco.

Connessioni seriali punto-punto:
- i protocolli HDLC e PPP e configurazione del PPP sui router.

Introduzione alle reti ed i servizi Frame Relay:
- tipi di LMI ed Incapsulamento
- configurazione di Frame Relay tra sito centrale e siti periferici.

NAT (Terminologia, NAT statico e dinamico).

Introduzione ad IPv6:
- caratteristiche generali e differenze rispetto ad IPv4
- introduzione ai protocolli di routing per IPv6 ed alla loro configurazione su router Cisco
- cenni sui principali meccanismi di transizione.

Introduzione alle Wireless LAN:
- principi fondamentali; apparati, componenti e parametri di configurazione delle WLAN.

Aspetti generali di sicurezza delle Reti IP.

Obiettivi
Comprendere la struttura ed i meccanismi base di funzionamento di reti IP in ambiente LAN e WAN.
Saper Utilizzare i comandi di base del sistema operativo Cisco (IOS).
Saper configurare, gestire ed effettuare il troubleshooting di reti Cisco in ambito LAN e WAN di piccole e medie dimensioni.

Destinatari
Tecnici di rete ed operatori di help desk che operino nel settore del networking, o ad altre figure professionali che abbiano bisogno di acquisire competenze introduttive di buon livello sulla configurazione e la gestione di router e switch cisco.

Prerequisiti
Conoscenze di base sull'utilizzo di Personal Computer e dei servizi Internet, sulle reti LAN, sull'architettura TCP/IP, e conoscenze introduttive sul routing IP.

Routing IP nell'IOS Cisco

Il corso affronta il tema generale del Routing IP e descrive i più importanti protocolli di routing utilizzati nelle reti di medie e grandi dimensioni. In particolare, vengono analizzati i protocolli di routing Distance Vector e Link State e fornite informazioni approfondite sui protocolli interni (EIGRP e OSPF) ed inter-dominio (BGP). Sono anche trattate in dettaglio le problematiche di redistribuzione tra protocolli di routing e di filtraggio degli annunci e problematiche di sicurezza sia dei router che dei protocolli di routing.
La descrizione teorica degli argomenti trattati è completata da una rilevante attività *hands on* su un ricco laboratorio, costituito da router Cisco che riproduce situazioni analoghe a quelle reali.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 300-101 "ROUTE v2.0".

Agenda (5 giorni)





Principi di routing:

- fondamenti (metrica, grado di preferenza, tabelle di routing).
- protocolli di routing Distance Vector (DV) e Link State (LS).

Il protocollo RIPng (RIP per IPv6).

Il protocollo EIGRP:

- aspetti di base: funzionamento, messaggi, metriche, algoritmo DUAL
- aspetti di scalabilità e sicurezza
- configurazione di base e troubleshooting nell'IOS Cisco
- EIGRP per IPv6.

Il protocollo OSPF:

- richiami sull'impiego di OSPF in area singola
- tipi di router, LSA, aree
- configurazione di OSPF multiarea nell'IOS Cisco
- aspetti avanzati di OSPF: aggregazione, virtual-link, sicurezza, OSPF su reti NBMA
- OSPFv3: differenze con OSPFv2 e configurazione.

Meccanismi di Path Control: redistribuzione, filtraggio, distanza amministrativa, CEF switching, Policy Based Routing.

Connettività Clienti-Internet:

- connessioni Single-Homed IPv4 e IPv6
- connessioni fault-tolerant
- vantaggi dell'utilizzo del protocollo BGP.

Routing inter-dominio: il protocollo BGP:

- funzionamento di base, sessioni e attributi BGP, processo di selezione
- implementazione base nell'IOS Cisco
- filtraggio degli annunci: filtri inbound/outbound, prefix-list, utilizzo delle route-map
- politiche di routing: il processo di selezione nei router Cisco, gestione del traffico outbound e inbound
- BGP per IPv6.

Aspetti di sicurezza dei router e dei protocolli di routing.

Obiettivi

Al termine del corso i partecipanti:

- conosceranno i meccanismi di funzionamento dei protocolli di routing IP e la loro interazione nelle reti
- conosceranno l'implementazione in ambiente Cisco dei protocolli intra-dominio (EIGRP e OSPF), e inter-dominio (BGP) sia in ambiente IPv4 che IPv6
- sapranno progettare e effettuare configurazioni di scenari complessi di rete.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Conoscenze dell'architettura TCP/IP e dei principi del routing. Inoltre risultano utili conoscenze sulla configurazione di apparati Cisco, configurazione di route statiche e di protocolli base (RIP, EIGRP, OSPF in area singola), configurazione di interfacce seriali per linee dedicate ed accessi Frame Relay, configurazione di liste di accesso standard ed estese, utilizzo dei comandi show e debug.

Routing IP nell'IOS XR Cisco

Il corso fornisce le competenze operative sulla configurazione base ed avanzata dei protocolli di routing IP negli apparati Cisco *carrier-grade*, che utilizzano il sistema operativo IOS XR. Il corso focalizza l'attenzione sui principali protocolli di routing utilizzati nelle reti dei *Service Provider* (OSPF, IS-IS, BGP). È prevista una rilevante attività di laboratorio *hands on,* costituito da router Cisco basati su IOS XR e IOS.

Agenda (3 giorni)



Routing nelle reti ISP:

- ruolo di OSPF e IS-IS
- ruolo del BGP
- interazione tra protocolli IGP e BGP.

OSPF: aspetti base ed avanzati:

- richiami sui fondamenti del protocollo OSPF
- OSPF multiarea
- aspetti avanzati: LSA, tipi di aree, *route summarization*, *virtual link*
- configurazioni base ed avanzate in ambiente IOS XR.

IS-IS: aspetti base ed avanzati:

- richiami sui fondamenti del protocollo IS-IS
- IS-IS multilivello
- redistribuzione e *Route Leaking*
- configurazioni base ed avanzate in ambiente IOS XR.

BGP: aspetti base ed avanzati:

- richiami sui fondamenti del protocollo BGP
- aggregazione e filtraggio dei prefissi
- Routing Policy e Route Policy language
- politiche di routing *inbound/outbound*
- meccanismi di scalabilità (*Route Reflection*, Confederazioni BGP)
- configurazioni base ed avanzate in ambiente IOS XR.

Meccanismi di *Path Control:*

- redistribuzione tra protocolli di routing
- filtraggio
- manipolazione della distanza amministrativa.

Obiettivi

Al termine del corso i partecipanti saranno in grado di configurare in ambiente IOS XR, gli aspetti base ed avanzati dei principali protocolli di routing utilizzati nelle reti dei Service Provider (OSPF, IS-IS, BGP).

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider e Enterprise di medie/grandi dimensioni.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nel corso “Routing IP nell'IOS CISCO” (INP232).



Troubleshooting di reti Cisco

Il corso fornisce competenze operative utili ad effettuare operazioni di baselining e troubleshooting in ambienti di rete locale e geografica basati su apparati Cisco. Dopo una panoramica sui criteri generali e sulle modalità di troubleshooting, è proposta una metodologia standard per la risoluzione dei malfunzionamenti.
Durante il corso saranno proposti ai partecipanti numerosi casi di studio, per un totale di oltre 50 'ticket' da risolvere. I casi di studio saranno svolti in un ambiente di rete 'reale' (non simulato) sul quale, a partire da configurazioni predefinite affette da malfunzionamenti, i partecipanti dovranno applicare le metodologie di problem solving illustrate nella parte teorica del corso. Nella prima parte del corso gli scenari proposti sono organizzati in funzione delle diverse tecnologie e, per ciascuna di esse, verranno fatti dei brevi richiami teorici. Nella parte finale del corso gli scenari proposti sono invece ottenuti mettendo assieme problemi di natura diversa, con complessità di risoluzione via via crescente.
Il corso è parte del percorso formativo raccomandato per ottenere la certificazione Cisco Certified Network Professional Routing and Switching (CCNP R&S) e fornisce le competenze necessarie per sostenere il nuovo esame di certificazione Cisco 'TSHOOT versione 2' (Esame Cisco 300-135).

Agenda (5 giorni)





Processi e strumenti per il troubleshooting:

- introduzione al Troubleshooting
- accesso al Cisco Connection On-line (CCO)
- strumenti disponibili sul Technical Assistance Center (TAC).

Le metodologie di Troubleshooting:

- un metodo sistematico e strutturato di troubleshooting
- isolamento dei malfunzionamenti
- il troubleshooting come componente della "manutenzione".

Gli strumenti di analisi sul software IOS:

- processi di routing e switching
- tracciamento dei flussi di traffico nei router
- il filtraggio e la redirezione degli output di IOS
- comandi di trace, ping, show e debug.

Troubleshooting di Reti di Campus e di VLAN:

- strumenti di troubleshooting sugli switch catalyst
- i catalyst ed il protocollo di Spanning Tree
- risoluzione di problemi di VTP
- identificazione e risoluzione dei problemi sulle VLAN e sui Trunk.

Troubleshooting di First Hop Redundancy in IPv4 ed IPv6:

- troubleshooting di HSRP, VRRP e GLBP.

Troubleshooting del routing in reti TCP/IP:

- identificazione dei problemi di connettività a livello di rete
- troubeshooting di connettività IPv4 ed IPv6
- troubleshooting dei protocolli di routing per IPv4 ed IPv6: RIPng, EIGRP, OSPF, OSPFv3, Multiprotocol BGP
- monitoraggio delle prestazioni dei Router.

Troubleshooting di soluzioni di sicurezza:

- AAA, Tacacs e Radius
- sicurezza L2
- sicurezza in IPv4 e sicurezza in IPv6
- sicurezza dei protocolli di routing.

Troubleshooting di reti Cisco

Obiettivi

Al termine del corso i partecipanti sapranno:

- utilizzare metodologie e strumenti standard per la risoluzione di problemi e malfunzionamenti di rete
- utilizzare al meglio i comandi diagnostici del Cisco IOS per l'analisi di dati e per la valutazione di potenziali problemi di rete o di apparato
- effettuare operazioni di troubleshooting su reti Cisco di media e grande dimensione.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Per poter trarre pieno beneficio dal corso, è richiesta una conoscenza generale delle reti IP e esperienza di configurazione dei router Cisco.



Cisco Nexus 7000 Switch per Data Center

A fronte dei cambiamenti di strategia di Cisco, per avere un numero consistente di porte a 10 Gb/s è necessario impiegare gli apparati Nexus. Pertanto diventa fondamentale avere una conoscenza dell'architettura del Nexus e soprattutto del set di comandi che è abbastanza differente dall'IOS. Inoltre gli Switch della serie Nexus hanno la possibilità di collegare degli Extender ed hanno anche un nuovo approccio su come realizzare collegamenti aggregati attraverso il Virtual Port Channel.
Il corso, in collaborazione con b!, prevede un'intensa attività di laboratorio.

Agenda (3 giorni)



Cisco Nexus 7000 switch Product Overview.

Cisco Nexus 7000 Switch Feature Configuration.

Configure the Nexus 7000 in Converged Network Environments.

Understand the Nexus 7000 System Hardware and Software Architecture.

Review the Nexus 7000 Software Features and Licensing.

Understand the Nexus 7000 High-Availability Features.

Fibre Channel over Ethernet (FCoE) on the Cisco Nexus 7000 switch.

Configure the Nexus 7000 Management and Monitoring Features.

Understand the Relationship Between the Nexus 7000 and 5000 Product Families.

Configure Advanced Features Including Congestion Avoidance, Traffic Management, Static and Dynamic Pinning.

Utilize the Fabric and Device Manager Products to Perform Discovery, Configuration, Management and Troubleshooting.

Laboratorio

Nexus 7000 Hardware Discovery and System Management.

Configure the Nexus 7000 for Dual-Homing Using the Virtual Port-Channel Feature.

Configurare il VPC.

Configurare le VLAN e lo Spanning tree.

Configurare il VLAN Routing.

Configurare l'HSRP.

Configure Nexus 7000 Traffic Management and QoS and Monitor FCoE Performance Using Ethanalyzer and SPAN with Wireshark.

Configure Nexus 7000 Security Features.

Configure ACLs.

Obiettivi

Il corso fornisce le conoscenze necessarie per la configurazione e gestione degli Switch Cisco Nexus 7000 per il Data Center.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Buona esperienza di configurazione su Switch catalyst e delle configurazioni di routing.

Configurazione, esercizio e manutenzione dei router Cisco Hi-End con sistema operativo IOS-XR

Cisco sta rapidamente adottando il suo sistema operativo di nuova generazione, l'IOS-XR, nelle proprie piattaforme di routing Carrier-Class, come i CRS, gli ASR 9000 e gli XR-12000.
Il corso descrive le principali funzionalità di esercizio e manutenzione dei router Cisco con IOS-XR, la configurazione delle principali funzionalità legate all'operatività dei router con IOS-XR nella core-network e nell'accesso delle reti ISP o in reti 'Enterprise' di grande e grandissima dimensione.
La formazione d'aula è integrata da una importante componente operativa di laboratorio svolta sui router XR-12000. Nelle esercitazioni i partecipanti, singolarmente o in piccoli gruppi da due persone, potranno configurare tutte le principali funzionalità trattate nel corso in una rete che riproduce un ambiente ISP in cui si fanno interoperare apparati con IOS e con IOS-XR.

Agenda (3 giorni)



Le piattaforme Cisco con IOS XR:

- l'architettura fisica dei router Cisco CRS, ASR 9000 e XR-12000
  - chassis, Switch Fabric, Schede di linea, processori, alimentazione
  - l'ambiente operativo
  - manutenzione dell' hardware inventory
- il Sistema Operativo IOS-XR
  - architettura del sistema operativo
  - installazione e manutenzione del software
  - comprensione, monitoraggio e risoluzione dei problemi e processi di memoria
  - introduzione alla configurazione del IOS XR e differenze con l' IOS.

Il piano di controllo del Cisco IOS XR:

- configurazione e gestione dei protocolli di routing IGP
  - configurazione di indirizzamento IP4 e IPv6
  - configurazione del routing statico per IPv4 e IPv6
  - configurazione base di OSPFv2 e OSPFv3
- configurazione e gestione del BGP
  - configurazioni di sessioni BGP per IPv4 e IPv6
  - configurazione delle address family IPv4 ed IPv6
  - gestione delle politiche di routing
- protezione del piano di controllo
  - introduzione alla protezione del Piano di Controllo su IOS-XR
  - Local Packet Transport Services (LPTS)
  - Exceptions Packet Rate-Limiters.

Il piano dati del Cisco IOS XR:

- Implementazione del packet forwarding sulle architetture Cisco Carrier Grade
  - inoltro
  - Packet Filtering
  - QoS
  - NetFlow.

Il Piano di Gestione del Cisco IOS XR:

- introduzione al Piano di Gestione nel Cisco IOS XR
- gestione dell'accesso remoto e SNMP
- gestione dei Secure Domain Router (SDR) con il Cisco IOS XR.

Obiettivi

Al termine del corso i partecipanti saranno in grado di configurare e manuterere i Router Cisco con sistema operativo IOS-XR.

Destinatari

Progettisti, system engineer, personale di supporto tecnico, ed in genere a professionisti del settore che hanno bisogno di conoscere le caratteristiche e la configurazione dei router Cisco con IOS-XR.

Prerequisiti

Conoscenze di base sull'interworking IP (architettura TCP/IP, routing, switching, ecc.). Discreta esperienza nell'installazione, nella configurazione e troubleshooting di router Cisco con IOS.



Strumenti Open Source per il Network Management

Nelle reti IP di grandi dimensioni è essenziale poter disporre di strumenti evoluti di Network Management, in grado di semplificare e rendere più efficiente l'esercizio della rete e degli apparati che la costituiscono.
Per far fronte alle innumerevoli difficoltà che un network manager si trova ad affrontare nella quotidiana gestione di una rete IP, i costruttori mettono a disposizione una grande quantità di strumenti applicativi specificamente progettati per la gestione dei propri dispositivi. Le soluzioni proposte dai vendor di apparati hanno però quasi sempre costi molto elevati, tali da renderle idonee esclusivamente alla gestione di reti di grandi dimensioni. In molti casi strumenti Open Source di Network Management possono costituire una valida ed economica alternativa.
Il corso fornisce un'introduzione alle problematiche di network management, descrive i principali standard coinvolti e le principali applicazioni oggi utilizzate e prevede, oltre alla descrizione teorica degli argomenti trattati, dimostrazioni in laboratorio su sistemi di Network Management Open Source.

Agenda (3 giorni)



Overview sul Network Management:

- definizioni e requirements
- le aree di Network Management secondo OSI
- dispositivi e raccolta delle informazioni
- architetture e sistemi per il Network Management
- il modello Manager/Agent/managed Object.

Protocolli e Standard:

- le basi del protocollo SNMP
- il Management Information Base (MIB)
- MIB2 e MIB proprietari
- RMON ed RMON2
- i messaggi SNMP
- sicurezza SNMP e community
- SNMP versione 2c e versione 3.
- Il protocollo Netflow ed il Netflow monitoring
- l'Internet Protocol Flow Information eXport (IPFIX).

Cenni su alcune applicazioni commerciali di Netwok Management:

- HP Openview Network Node Manager
- Cisco Works e le Network Analysis Module (NAM).

I linguaggi di scripting ed il loro utilizzo nel Network Management:

- richiami sui linguaggi PERL e Visual Basic
- il Comprehensive Perl Archive Network (CPAN)
- esempi di script in PERL per la gestione di apparati di rete
- utilizzo del PERL per accedere a variabili del MIB SNMP.

Alcuni Strumenti Open Source di Network Management:

- Multi Router Traffic Grapher (MRTG)
- NetXMS
- Nagios
- Icinga
- OpenNMS.

Strumenti Open Source per il Network Management

Obiettivi

Al termine del corso i partecipanti:

- saranno in grado di riconoscere le principali criticità che si incontrano nella gestione delle reti IP
- avranno acquisito una panoramica di ampio spettro e di livello approfondito sui metodi e sulle principali tecnologie per la gestione delle reti e dei sistemi
- conosceranno il funzionamento del protocollo SNMP e sapranno valutare le differenze prestazionali e di sicurezza tra le diverse versioni
- avranno una visione d'insieme delle funzionalità di gestione rese disponibili da piattaforme di Network Management
- conosceranno le caratteristiche funzionali delle principali applicazioni Open Source per il Network Monitoring e Management
- disporranno degli strumenti di base per scrivere ed utilizzare 'script' dedicati alla automazione delle operazioni di gestione.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili e tecnici di Provisioning e Operation.

Prerequisiti

Una buona conoscenza di base sulle reti LAN e sull'architettura TCP/IP.

BGP: aspetti base

Il corso fornisce competenze teoriche e pratiche di base sul protocollo BGP, descrive nel dettaglio i problemi di indirizzamento, routing e connettività in Internet, nonché le funzionalità del BGP, la sua configurazione su router Cisco e Juniper e le metodologie di troubleshooting. È prevista una rilevante attività *hands on* su un ricco laboratorio, costituito da router Cisco e Juniper.
Nel corso sono trattati argomenti utili per la preparazione alle certificazioni Cisco CCNP R&S e Juniper JNCIS-SP e JNCIP-SP.

Agenda (3 giorni)





Concetti fondamentali:

- Autonomous System
- tipologie di connettività tra AS
- funzionamento di base
- sessioni e attributi BGP
- processo di selezione e politiche di routing.

Implementazione base nell'IOS Cisco e nel JUNOS Juniper

Aggregazione dei prefissi:

- scenari di aggregazione
- aggregazione con e senza memoria.

Politiche di routing:

- filtraggio dei prefissi
- gestione del traffico inbound/outbound
- applicazioni alla Connettività Clienti-ISP
- aspetti di configurazione nei router Cisco e Juniper.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- gli strumenti per la configurazione e gestione di reti che utilizzano il protocollo BGP in varie situazioni (Reti ISP, Reti aziendali multi-homed, AS di transito, peering con altri AS)
- i criteri di pianificazione e realizzazione di progetti di rete basati sul protocollo BGP
- l'implementazione di base del BGP nell'IOS Cisco e nel JUNOS Juniper.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Per poter trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP, in particolare del routing IP e qualche esperienza di configurazione base dei router Cisco e/o Juniper.



BGP: aspetti avanzati

Il corso fornisce competenze teoriche e pratiche avanzate sul protocollo BGP e prevede una rilevante attività *hands on* su un laboratorio costituito da router Cisco e Juniper, nel quale sono riprodotte situazioni analoghe a quelle reali. Sono presentati anche dei Case Studies di configurazioni su router in produzione. Il corso IPN247 e l'IPN246, che tratta gli aspetti di base, consentono la piena conoscenza dei temi legati al protocollo BGP.
Nel corso sono trattati temi utili per sostenere gli esami di certificazione Cisco CCNP-SP, CCIE Routing & Switching e Service Provider e di certificazione Juniper JNCIS-SP, JNCIP-SP e JNCIE-SP.

Agenda (3 giorni)





Richiami sui concetti fondamentali del protocollo BGP.

Aspetti avanzati di filtraggio e politiche di routing:

- regular expression
- filtri basati sull'attributo community
- gestione avanzata dell'attributo MED
- politiche di routing basate sull'attributo community.

Architetture e meccanismi per la Scalabilità:

- architetture di Route Reflection
- confederazioni BGP (cenni)
- Outbound Route Filtering (ORF).

Meccanismi di Stabilità:

- Graceful Restart
- Route Flap Damping.

Aspetti di sicurezza:

- autenticazione dei messaggi
- limitazione del numero di prefissi ricevuti.

Il BGP nelle reti enterprise:

- tipologie di connettività clienti-ISP
- load balancing del traffico
- *Best Practice di configurazione.*

Il BGP nelle reti dei Service Provider:

- architettura di routing delle reti degli ISP
- convergenza IGP/BGP
- *Best Practice di configurazione.*

Obiettivi

Al termine del corso i partecipanti conosceranno:

- gli aspetti avanzati del protocollo BGP come le politiche di filtraggio e routing, i meccanismi di scalabilità, stabilità e sicurezza del protocollo
- le best-practice di implementazione nelle reti enterprise e nelle reti dei service provider.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Sono richieste conoscenze di base del protocollo BGP e alcune esperienze di configurazione base dei router Cisco e/o Juniper.



Routing Multicast

La diffusione di nuovi servizi multimediali sulle reti IP rende nuovamente attuali le problematiche di instradamento di flussi multicast. La modalità di comunicazione unicast non è infatti efficiente nel supporto di applicazioni di broadcasting, come, ad esempio, la diffusione di contenuti video su larga scala, come l'IPTV, o di servizi multicasting, come la videoconferenza e tutte le applicazioni che ne derivano (telelavoro, telemedicina, e-learning, ecc.). L'adozione delle tecniche di trasporto multicast in applicazioni che prevedono la distribuzione da una o più sorgenti verso destinatari multipli, consente di sfruttare al meglio la capacità della rete, rendendo di fatto possibili applicazioni che, se veicolate in unicast, porterebbero rapidamente alla saturazione delle risorse. Il corso fornisce competenze teorico-pratiche sul multicast IP e capacità operative sulla configurazione del multicast su apparati di rete. Oltre alla descrizione teorica degli argomenti trattati è prevista, infatti, una rilevante attività di laboratorio con apparati Cisco in un ambiente che riproduce in piccola scala una rete multicast reale.

Agenda (3 giorni)



Introduzione al Routing Multicast: (motivazioni e applicazioni; indirizzi Multicast).

Il protocollo IGMP:

- IGMPv1, IGMPv2 e IGMPv3
- interoperabilità IGMPv1/IGMPv2/IGMPv3.

Il Multicast negli Switch:

- generalità; cenni su GMRP e CGMP; IGMP snooping.

Protocolli di routing multicast:

- forwarding dei pacchetti multicast e Reverse Path Forwarding (RPF)
- alberi multicast; protocolli dense-mode; protocolli sparse-mode.

Il protocollo PIM:

- aspetti di base;
- PIM-DM (Dense Mode) e PIM-SM (Sparse Mode)
- metodi per la selezione del RP (Rendezvous Point).

Modelli di servizio basati sul protocollo PIM:

- Source-Specific Multicast (SSM)
- PIM Bidirezionale (PIM-Bidir).

Routing Multicast Interdominio (cenni):

- scenario, problemi e soluzioni; ruolo del protocollo MP-BGP; il protocollo MSDP.

Cenni sul Multicast per IPv6:

- il formato degli indirizzi IPv6
- il multicast per IPv6 e le principali differenze rispetto al multicast in IPv4
- il protocollo MLD, MLDv2 e MLD snooping.

Laboratorio: Configurazione di reti multicast su router Cisco.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- comprendere i meccanismi di funzionamento del routing multicast in ambiente IP
- progettare l'applicazione di funzionalità di routing multicast ad una rete IP
- configurare funzionalità di routing multicast su router e su switch L3 Cisco
- ottimizzare il supporto al multicast su switch Cisco L2
- mettere in sicurezza le funzionalità multicast.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Conoscenza delle reti IP ed esperienza di configurazione dei router Cisco per ciò che riguarda indirizzi IP, protocolli di routing, liste di accesso standard ed estese.

Introduzione alla Configurazione di Router Juniper

Il corso fornisce conoscenze teoriche e competenze operative sulla configurazione base dei dispositivi Juniper Networks serie J, M e T che utilizzano il sistema operativo JUNOS, e mira all'acquisizione di una buona manualità nella configurazione dei dispositivi Juniper, attraverso, una rilevante attività di laboratorio *hands on*.

Il corso fornisce le competenze necessarie per sostenere l'esame JN0-102 per la certificazione Juniper JNCIA-Junos.

Agenda (3 giorni)





Architettura Hardware e Software:

- router Juniper (serie J, M, T)
- Control Plane e Data Plane
- Routing Engine e Forwarding Engine
- processo di avvio di un router Juniper.

L'ambiente shell:

- gestione utenti ed account.

La CLI nel JUNOS:

- gli ambienti Operational Mode e Configuration Mode
- gestione di utenti (classi di login ed account)
- comandi di configurazione in ambiente Configuration Mode
- concetti fondamentali e configurazione.

Firewall Filter.

Routing Policy e Route Filter.

Fondamenti di routing IP nel JUNOS:

- routing statico e dinamico
- il protocollo RIP
- OSPF in area singola.

Classi di servizio e QoS IP nel JUNOS.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- l'architettura HW e SW dei router Juniper
- l'uso dell'interfaccia di configurazione CLI dei router Juniper
- la configurazione delle funzionalità di base dei router Juniper.

Destinatari

Amministratori e tecnici di rete responsabili dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente Juniper. Rientra nel percorso di certificazione Juniper JNCIA.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale dell'architettura TCP/IP.



Routing IP nel JUNOS Juniper: aspetti di base

Il corso fornisce le conoscenze teoriche di base e le competenze operative sulla configurazione base dei principali protocolli di routing nei dispositivi Juniper Networks serie J, M e T che utilizzano il sistema operativo JUNOS. È prevista una rilevante attività di laboratorio *hands on,* costituito da router Juniper interconnessi con una rete Cisco.
È parte del programmi di certificazione Juniper JNCIS-SP e Juniper JNCIS-ENT.





Agenda (3 giorni)

Introduzione al routing IP:

- routing statico
- Aggregate Routes, Generated Routes e Contributing Routes.

Introduzione al routing Dinamico: il Protocollo RIP.

Il protocollo OSPF:

- richiami sui concetti base
- configurazione in ambiente JUNOS
- comandi show e traceoptions.

Il protocollo IS-IS:

- richiami sui concetti base
- configurazione in ambiente JUNOS
- comandi show e traceoptions.

Il protocollo BGP:

- aspetti fondamentali: sessioni, attributi, politiche di routing
- configurazione in ambiente JUNOS
- comandi show e traceoptions.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- configurare i principali protocolli di routing (route statiche, RIP, OSPF, IS-IS, BGP)
- valutare i problemi di interlavoro con i router Cisco.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nel corso "Introduzione alla Configurazione di Router Juniper" (INP252).

Routing IP nel JUNOS Juniper: aspetti avanzati

Il corso fornisce le conoscenze teoriche e le competenze operative sulla configurazione avanzata dei protocolli di routing nei dispositivi Juniper Networks serie J, M e T, che utilizzano il sistema operativo JUNOS. È prevista una rilevante attività di laboratorio *hands on,* costituito da router Juniper interconnessi con una rete Cisco.

Il corso è parte dei programmi di certificazione Juniper JNCIP-SP e JNCIE-SP.

Agenda (4 giorni)





Aspetti avanzati di configurazione delle Routing Policy JUNOS.

OSPF:

- richiami sui fondamenti del protocollo OSPF
- aspetti avanzati: LSA, tipi di aree, Route-Summarization, Virtual Link
- configurazioni avanzate in ambiente JUNOS.

IS-IS:

- richiami sui fondamenti del protocollo IS-IS
- IS-IS multilivello
- redistribuzione e *Route Leaking*
- configurazione avanzate in ambiente JUNOS.

BGP:

- richiami sui fondamenti del protocollo BGP
- aggregazione e filtraggio dei prefissi
- inbound e outbound Route Filtering,
- politiche di routing *inbound/outbound*
- meccanismi di scalabilità (*Route Reflection*, Confederazioni BGP)
- configurazione avanzate in ambiente JUNOS.

Routing IPv6 nel JUNOS:

- routing statico
- estensioni di IS-IS per IPv6
- OSPFv3
- BGP per IPv6.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- descrivere gli aspetti avanzati di OSPF, IS-IS e BGP e il loro ruolo nelle reti dei Service Provider
- configurare gli aspetti avanzati dei principali protocolli di routing (OSPF, IS-IS, BGP).

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Candidati al conseguimento della certificazione Juniper JNCIP-SP.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "Routing IP nel JUNOS Juniper: aspetti di base" (IPN253).

Routing multicast nel JUNOS Juniper

Il corso fornisce competenze teorico-pratiche sul multicast IP e le capacità operative sulla configurazione del multicast su apparati Juniper che adottano il sistema oprativo JUNOS. Oltre alla descrizione teorica degli argomenti trattati, è prevista una rilevante attività di laboratorio con apparati Juniper, nel quale sono riprodotte situazioni analoghe a quelle reali.
Il corso è parte del programma di certificazione Juniper JNCIP-SP.

Agenda (2 giorni)





Introduzione al Routing Multicast:

- motivazioni e applicazioni
- indirizzi Multicast.

Il protocollo IGMP.

Protocolli di routing multi cast:

- Forwarding dei pacchetti multicast
- Reverse Path Forwarding
- alberi multicast
- protocolli dense-mode e sparse-mode.

Il protocollo PIM:

- aspetti base
- PIM-DM (*Dense Mode*) e PIM-SM (*Sparse Mode*)
- implementazione di PIM-DM e PIM-SM nel JUNOS.

Metodi per la selezione del RP (Rendezvous Point)

- Auto-RP
- Bootstrap router
- Anycast-RP.

Modelli di servizio basati sul protocollo PIM

- Source-Specific Multicast (SSM)
- PIM Bidirezionale (PIM-Bidir).

Routing Multicast Interdominio (cenni).

- scenario, problemi e soluzioni
- il protocollo MSDP

Multicast per IPv6.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- descrivere il funzionamento dei principali protocolli di routing multicast e dei protocolli correlati
- configurare e monitorare nel JUNOS il protocollo PIM e le sue varianti

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JNCIP-SP.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "Routing IP nel JUNOS: aspetti base" (IPN 253).



Carrier Ethernet in ambiente Juniper

Il corso fornisce le conoscenze teoriche e operative avanzate sulla configurazione base ed avanzata servizi Carrier Ethernet in ambiente Juniper. Saranno trattati argomenti come i concetti base delle reti Switched Ethernet e Ethernet OAM e il processo di standardizzazione del Metro Ethernet Forum. Inoltre saranno affrontati argomenti avanzati come le implementazioni Junos di interfacce IRB, virtual switch, load balancing, Multiple VLAN Registration Protocol (MVRP), multichassis LAG (MC-LAG), ecc. .
Il corso è parte del programma di certificazione Juniper JNCIS-SP.

Agenda (2 giorni)





Carrier Ethernet:
- Ethernet reti metropolitane
- processo di standardizzazione (IEEE, IETF, MEF)
- funzioni L2 degli apparati Juniper della serie MX.

Fondamenti sulle reti switched Etherne:
- LAN e VLAN; configurazione, monitoraggio e amministrazione di VLAN
- Inter-VLAN routing: configurazione di interfacce IRB
- L2 Firewall Filter.

Virtual Switches:
- cenni sulle istanze di routing
- configurazione e monitoraggio di Virtual switch; interconnessione di istanze di routing.

Provider Bridging:
- Provider Bridging e Provider Backbone Bridging
- standard IEEE 802.1ad 802.1ah
- configurazione e monitoraggio di Provider Bridging.

Il protocollo Spanning-Tree e le sue varianti:
- richiami su STP; varianti di STP: RSTP, MSTP, VSTP
- configurazione e monitoraggio di STP, RSTP, MSTP, VSTP
- BPDU, Loop, Root Protection.

Ethernet OAM:
- Standard IEEE 802.1ag
- LFM e CFM
- configurazione e monitoraggio di Ethernet OAM.

High Availability:
- cenni sulla funzionalità di Ethernet Ring Protection (ERP)
- configurazione e monitoraggio di ERP
- cenni sui Link Aggregation Group (LAG)
- LAG multi chassis; configurazione e monitoraggio di LAG.

Obiettivi
Al termine del corso i partecipanti saranno in grado di:
- descrivere i principali servizi Carrier Ethernet e valutarne i pro e contro
- configurare reti e servizi Carrier Ethernet in ambiente Juniper.

Destinatari
Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JNCIS-SP.

Prerequisiti
Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP e delle reti Switched Ethernet: indirizzi IP, protocolli di routing fondamentali, VLAN, inter-vlan routing, e avere le conoscenze sui temi trattati nel corso "Introduzione alla Configurazione di Router Juniper" (INP252).

Switching nel JUNOS Juniper

Il corso fornisce competenze di livello intermedio sullo Switching Ethernet nelle reti Enterprise in ambiente JUNOS. Dopo una panoramica sui concetti di base e sui meccanismi di funzionamento degli switch di livello 2 e multilayer, descrive i meccanismi di Virtual LAN (VLAN), il protocollo di Spanning Tree Protocol (STP), le funzioni di sicurezza di livello 2 e livello 3, ed i meccanismi di alta disponibilità.
È prevista una rilevante attività di laboratorio *hands on,* costituito da switch Juniper della serie EX, attraverso la quale gli studenti acquisiranno esperienza nella configurazione e nel monitoraggio del sistema operativo Junos.
Il corso, insieme al corso IPN253, fornisce le competenze necessarie per sostenere l'esame JN0-343 per la certificazione Juniper JNCIS-ENT.

Agenda (3 giorni)





Reti *switched* di Livello 2:

- aspetti di base
- Bridging e Switching
- funzionamento degli Switch
- Virtual LAN e inter-VLAN routing
- Voice VLAN
- Link Aggregation Group
- configurazioni di base degli switch della famiglia *Juniper EX*
- laboratorio 1: configurazioni di base, VLAN e *trunk, Link Aggregation.*

Il protocollo di *Spanning-Tree*:

- concetti fondamentali e standard IEEE 802.1d
- Rapid Spanning-Tree e IEEE 802.1w
- meccanismi di protezione dello Spanning Tree: BPDU protection, Root protection e Loop protection
- cenni su Multiple Spanning Tree (MST IEEE 802.1s) e VLAN Spanning Tree (VSTP)
- configurazione dello Spanning Tree su switch Juniper EX
- laboratorio 2: configurazione e monitoring di STP, RSTP e meccanismi di protezione.

Aspetti di sicurezza e Firewall Filters:

- MAC limiting
- DHCP snooping
- Dynamic ARP inspection
- IP source guard
- meccanismi di Storm Control
- Firewall Filter
- laboratorio 3: meccanismi di sicurezza.

Meccanismi di High Availability:

- generalità sui meccanismi di ridondanza ed alta disponibilità
- Redundant Trunk Group
- Virtual Chassis
- ridondanza del *First Hop* e protocollo VRRP
- laboratorio 4: RTG, Virtual Chassis, VRRP.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- configurare reti di livello 2 e multilayer realizzate con apparati Juniper EX
- mettere in sicurezza reti Juniper utilizzando i meccanismi descritti nel corso
- scegliere e configurare i meccanismi di disponibilità disponibili sulla famiglia di switch EX.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JNCIS-ENT.

Switching nel JUNOS Juniper

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi “Introduzione alla Configurazione di Router Juniper” (INP252) e “Routing IP nel JUNOS Juniper: aspetti di base” (IPN253).



MPLS nel JUNOS Juniper

Il corso fornisce le conoscenze teoriche e le competenze operative avanzate sulla configurazione base ed avanzata di MPLS nei dispositivi Juniper Networks serie J, M e T, che utilizzano il sistema operativo JUNOS. Saranno trattati, oltre ai concetti e protocolli fondamentali di MPLS, tutti i principali servizi MPLS, come ad esempio, Traffic Engineering, L3VPN e L2VPN. È prevista una rilevante attività di laboratorio *hands on,* costituito router Juniper interconnessi con una rete Cisco.
Il corso è parte del programma di certificazione Juniper JNCIS-SP.

Agenda (5 giorni)





Motivazioni e servizi MPLS.

Concetti fondamentali:

- componenti funzionali
- Label Switched Paths
- protocolli per la Distribuzione delle etichette: LDP, RSVP-TE, BGP
- gestione del campo TTL.

Implementazione base di MPLS nel JUNOS:

- configurazione base
- configurazione del protocollo LDP
- Verifica e troubleshooting.

MPLS nelle reti ISP:

- architettura di routing delle reti ISP
- architettura di routing BGP/MPLS
- risoluzione del BGP *Next-Hop* nel JUNOS.

MPLS Traffic Engineering:

- concetti fondamentali
- costruzione del TE-LSDB
- determinazione dei percorsi
- segnalazione e gestione dei percorsi
- LSP Point-to-Multipoint.

Configurazione tunnel MPLS-TE nel JUNOS Juniper:

- configurazioni base
- configurazione di LSP Point-to-Multipoint
- definizione di vincoli
- configurazione del protocollo RSVP-TE
- verifica dello stato dei Tunnel
- integrazione con la Tabella di Routing.

Protezione del Traffico:

- modalità di protezione
- percorsi secondari
- protezione dei percorsi, Facility Backup, One-to-one Backup.

Reti Private Virtuali IP BGP/MPLS : aspetti base:

- generalità
- piano di controllo
- piano dati.

Implementazione JUNOS:

- configurazione di VPN *any-to-any*
- routing PE-CE
- verifica e troubleshooting
- topologia “Hub-and-Spoke”
- VPN Interprovider
- Servizi Carrier-of-Carriers.

Servizio multicast nelle VPN:
- Concetti fondamentali
- Next-generation multicast VPN
- implementazione JUNOS.

L2VPN basate su BGP:
- Provider-Provisioned L2VPN
- piano di controllo e piano dati
- implementazione JUNOS
- aspetti di scalabilità
- L2VPN e QoS.

L2VPN basate su LDP:
- piano di controllo e piano dati
- implementazione JUNOS
- Circuit Cross-Connect.

Il servizio VPL:
- piano di controllo basato su BGP
- piano dati
- Learning e Forwarding Process
- Implementazione JUNOS.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:
- configurare reti e servizi MPLS
- valutare i problemi di interlavoro con i router Cisco

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JNCIS-SP.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "Routing IP nel JUNOS" (IPN 253).

QoS IP nel JUNOS Juniper

Il corso fornisce competenze teorico-pratiche sulla QoS IP e sulla sua implementazione nel sistema oprativo JUNOS. Sono trattati tutti i blocchi funzionali della QoS IP, come classificazione, colorazione, controllo del traffico, scheduling, ecc. .
Il corso è parte del programma di certificazione Juniper JNCIP-SP.

Agenda (2 giorni)





Introduzione

- Qualità del Servizio nelle Reti a Commutazione di Pacchetto
- Indici di Qualità del Servizio
- Fattori che influenzano la QdS e possibili soluzioni

Il modello Differentiated Services (DiffServ)

- Architettura
- Per Hop Behaviour (PHB)

Classificazione e Colorazione del Traffico

- Tipi di classificatori
- Configurazione di classificatori di tipo BA
- Configurazione di classificatori di tipo MF
- *Rewrite rules* (Colorazione)

Controllo del Traffico

- Meccanismi di controllo
- L'algoritmo *Token Bucket*
- Traffic Policing

Implementazione dei PHB

- Meccanismi di *scheduling*
- Assegnazione delle *Forwarding Class* alle code
- Schedulers
- Configurazione di *RED drop profiles*

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- descrivere il funzionamento dei principali blocchi funzionali per l'applicazione della QoS IP
- configurare e monitorare nel JUNOS le funzionalità di QoS IP.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JNCIP-SP.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252).

Aspetti avanzati del Routing IP nelle reti Enterprise Juniper

Il corso fornisce le conoscenze teoriche e le competenze operative avanzate sulla configurazione avanzata dei protocolli di routing di interesse nelle reti *Enterprise*, nei dispositivi Juniper Networks serie J e M, che utilizzano il sistema operativo JUNOS. È prevista una rilevante attività di laboratorio *hands on,* su un laboratorio costituito da router Juniper interconnessi con una rete Cisco.
Il corso è parte del programma di certificazione Juniper JNCIP-ENT.

Agenda (3 giorni)





Aspetti avanzati di configurazione delle Routing Policy JUNOS.

OSPF:
- richiami sui fondamenti del protocollo OSPF
- aspetti avanzati: LSA, tipi di aree, Route-Summarization, Virtual Link
- configurazioni avanzate in ambiente JUNOS.

BGP:
- richiami sui fondamenti del protocollo BGP
- aggregazione e filtraggio dei prefissi
- inbound e outbound Route Filtering
- politiche di routing *inbound/outbound*
- meccanismi di scalabilità (*Route Reflection*)
- configurazioni avanzate in ambiente JUNOS.

Routing Multicast:
- indirizzi Multicast
- il protocollo IGMP
- protocolli di routing multicast
- PIM-DM (*Dense Mode*) e PIM-SM (*Sparse Mode*)
- PIM SSM
- implementazione di PIM-DM, PIM-SM e PIM SSM nel JUNOS.

QoS IP nel JUNOS:
- qualità del Servizio nelle Reti a Commutazione di Pacchetto
- il modello Differentiated Services (DiffServ)
- Classificazione e Colorazione del Traffico
- Traffic Policing
- Schedulers.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:
- descrivere gli aspetti avanzati di OSPF, BGP, Routing multicast e QoS IP e il loro ruolo nelle reti *Enterprise*
- configurare gli aspetti avanzati dei principali protocolli di routing di interesse nelle reti *Enterprise* (OSPF, BGP, Routing multicast)
- descrivere e configurare le principali funzionalità di QoS IP nel JUNOS.

Destinatari

Amministratori e tecnici di rete, responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente Enterprise.
Candidati al conseguimento della certificazione Juniper JNCIP-ENT.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "Routing IP nel JUNOS: aspetti base" (IPN253).



Aspetti avanzati delle Reti Switched Ethernet Juniper

Il corso fornisce conoscenze teoriche dettagliate e capacità operative avanzate sull'impiego di switch Juniper nelle reti *Enterprise.* In particolar modo sono descritte funzionalità avanzate di livello 2, i protocolli MST e VSTP, aspetti di autenticazione e controllo di accesso, meccanismi di QoS ed IP Telepnony, funzionalità di monitoring e troubleshooting. È prevista una rilevante attività di laboratorio *hands on,* su un ricco laboratorio didattico, costituito da switch Juniper della serie EX.
Il corso è parte del programma di certificazione Juniper JNCIP-ENT.

Agenda (2 giorni)





Aspetti avanzati dello Switching Ethernet:

- la gestione delle VLAN
- il GARP VLAN Registration Protocol (GVRP)
- il Multiple VLAN Registration Protocol (MVRP).

VPN di livello 2:

- generalità sul Tunnelling del livello 2 su reti Ethernet
- il Modello Q in Q ed il Layer 2 Protocol Tunnelling (L2PT).

Aspetti avanzati dello Spanning Tree:

- richiami sul RSTP
- il Multiple Spanning Tree Protocol (MST)
- il VLAN Spanning Tree Protocol (VSTP).

Autenticazione e Access Control:

- i meccanismi di Authentication, Authorization e Accounting (AAA)
- il protocollo Radius
- funzionalità ed utilizzo del protocollo IEEE802.1x
- il MAC Radius
- il Captive Portal.

IP Telephony:

- introduzione ad IP Telephony
- power over Ethernet (PoE) e lo standard IEEE802.3af
- impiego di LLDP nella connessione di telefoni IP ad uno switch
- le Voice VLAN ed il loro impiego.

Qualità del servizio a livello 2:

- il COS nelle trame IEEE802.1q
- classi di forwarding e Classsificazione delle trame
- tipi di policers e scheduling
- gestione del COS sugli switch della serie EX.

Monitoring e Troubleshooting:

- i più comuni problemi che possono impedire il corretto funzionamento della rete
- metodologie di analisi e risoluzione dei problemi
- strumenti di monitoring e troubleshooting disponibili sul Junos.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- gestire la configurazione centralizzata delle VLAN con GVRP ed MVRP
- configurare VSTP ed MST su apparati Juniper EX
- configurare funzionalità di controllo di accesso e sicurezza
- ottimizzare la rete per fornire servizi di IP Telephony
- configurare e gestire la QoS in reti Juniper di livello 2
- svolgere operazioni di monitoring e troubleshooting su apparati Juniper EX.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Enterprise di medie/grandi dimensioni. Candidati al conseguimento della certificazione Juniper JNCIP-ENT.

Aspetti avanzati delle Reti Switched Ethernet Juniper

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "Switching nel JUNOS Juniper" (IPN 258).

Multilayer Switching e Reti di Campus

Il corso descrive nel dettaglio le tecnologie di Switching impiegate nelle reti locali e metropolitane di medie e grandi dimensioni. Nella trattazione si fa principalmente riferimento alla progettazione, installazione ed amministrazione di Reti di Campus con l'impiego di tecnologie di switching multilayer Cisco. Ad integrazione della trattazione teorica, il corso prevede una rilevante attività di hands on su un ricco laboratorio, costituito da switch Cisco-Catalyst Layer 2 e Layer 3, che riproduce una rete di campus di grandi dimensioni.
Il corso fa parte del percorso proposto per conseguire la certificazione Cisco CCNP-R&S e fornisce le competenze necessarie per sostenere il nuovo esame di certificazione "Switch versione 2" (Esame Cisco 300-115).

Agenda (5 giorni)





Overview sulle reti di Campus:

- la struttura di una rete di campus ed il modello gerarchico: livelli di accesso, distribuzione e "core"
- architettura di reti di campus di piccole, medie e grandi dimensioni
- architetture di campus 'routed' e 'switched'.

Virtual LAN su apparati Catalyst:

- tipi di link e membership delle porte
- il protocollo 802.1q
- il VLAN Trunk Protocol (VTP v1, v2 e v3) ed il VPT pruning
- routing tra le VLAN
- considerazioni sulla progettazione: Local VLAN ed end-to-end VLAN.

Fast EtherChannel:

- caratteristiche ed utilizzo
- i protocolli LACP e PAgP.

LLDP e CDP:

- caratteristiche e differenze
- impiego e configurazione di LLDP.

Il protocollo dello Spanning Tree:

- richiami sullo STP, spanning tree singolo e "Per VLAN Spanning Tree"
- Rapid Spanning Tree Protocol (RSTP)
- Mutiple Spanning Tree Instance (MSTI) standard 802.1s.
- protezione dello spanning tree: BPDU guard, BPDU filtering, Root guard, Loop guard
- configurazione ed impiego di UDLD.

Multilayer switching:

- funzionalità degli switch multilayer
- tabelle di switching: CAM e Ternary CAM
- predisposizione degli switch ed SDM Templates
- porte switched, routed ed SVI.

DHCP:

- richiami sul protocollo
- DHCP relay
- configurazione del DHCP per IPv4 ed IPv6.

Tecnologie per la ridondanza del Default Gateway:

- Hot Standby Router Protocol (HSRP)
- Virtual Router Redundancy Protocol (VRRP)
- Gateway Load Balancing Protocol (GLBP)
- configurazioni ad elevata affidabilità
- HSRP e GLBP per IPv6.

Funzionalità di sicurezza e di protezione nelle reti switched:

- tipi di attacchi di livello 2 (MAC Flooding, DHCP Spoofing, VLAN Hopping, etc.)
- DHCP snooping, Dynamic ARP inspection, IP source Guard
- funzionalità AAA
- Port Security e IEEE 802.x
- Port ACL
- VLAN ACL e Private VLAN
- Storm Control.

Il Network Time Protocol (NTP):

- necessità di sincronizzazione
- versioni di NTP e SNTP
- NTP per IPv6.

Monitoring della Rete:

- il Simple Network Time Protocol (SNMP)
- le versioni v1, v2 e v3 e Configurazione di SNMPv3
- Netflow
- IP SLA
- SPAN ed RSPAN.

Virtualizzazione

- tecnologia Stackwise
- Supervisor Redundancy
- Virtual Switching System (VSS).

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- scegliere l'architettura di rete più idonea per reti locali e di campus, anche di grandi dimensioni
- scegliere gli apparati di switching più adatti nell'ambito delle famiglie di prodotti Cisco
- configurare switch Cisco di livello 2 e livello 3 anche in architetture di rete complesse
- configurare il supporto per le funzionalità di Voce su IP sugli switch Cisco
- svolgere attività di troubleshooting su reti LAN e di Campus
- mettere in sicurezza gli apparati di rete e configurare i meccanismi di sicurezza di livello 2.

Destinatari

Il corso è rivolto a tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Conoscenza generale delle reti IP ed esperienza di configurazione dei router Cisco.



Il Routing IP nelle Reti ISP: aspetti di base

Il corso fornisce le conoscenze teoriche e le capacità operative necessarie alla configurazione, alla verifica ed al *troubleshooting* dei protocolli di routing su reti '*carrier-grade*' in ambiente Cisco. Nel corso sono trattati i protocolli di routing IGP ed il BGP illustrandone la configurazione sui sistemi operativi Cisco IOS, IOS-XE, ed IOS-XR. La descrizione teorica degli argomenti trattati è completata da una rilevante attività *hands on* su un ricco laboratorio, costituito da router Cisco con sistema operativo IOS ed IOS-XR, che riproduce situazioni analoghe a quelle reali.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 642-883 "SPROUTE".

Agenda (5 giorni)





Il Routing nelle reti dei Service Provider:

- architettura delle reti ISP
- il ruolo di OSPF e IS-IS
- il ruolo del BGP
- interazione tra i protocolli IGP ed il BGP.

Il protocollo OSPFv2 ed OSPFv3:

- principi di base, messaggi, metriche
- OSPF multiarea
- Link State Advertisement
- tipi di aree: normali, stub, totally stubby ed NSSA
- Virtual Link
- aggregazione dei prefissi
- differenze tra OSPFv2 (per IPv4) ed OSPFv3 (per IPv6)
- implementazione nell'IOS, IOS-XE e IOS-XR.

Il protocollo IS-IS:

- principi di base, messaggi, metriche
- gli indirizzi OSI
- IS-IS multiarea in reti IPv4 ed IPv6
- Route Leaking
- Link State Packet
- implementazione nell'IOS, IOS-XE e IOS-XR.

Introduzione al protocollo BGP:

- l'architettura di routing di Internet
- funzionamento di base del BGP
- sessioni, messaggi ed attributi
- il processo di selezione
- le politiche di routing.

Implementazione del BGP nell'IOS, IOS-XE e IOS-XR:

- configurazioni base
- Route-map e Routing Policy
- Route Policy language
- controllo della configurazione e Troubleshooting di base
- filtraggio dei prefissi.

Politiche di routing:

- il processo di selezione nei router Cisco
- gestione del traffico outbound attraverso il parametro Weight
- gestione del traffico outbound attraverso l'attributo Local Preference
- gestione del traffico inbound attraverso l'attributo MED
- gestione del traffico inbound attraverso AS_PATH prepending.

Meccanismi di Path Control:

- redistribuzione tra protocolli di routing
- filtraggio
- manipolazione della distanza amministrativa
- Policy Based Routing.

Il Routing IP nelle Reti ISP: aspetti di base

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- comprendere i principi che governano il routing in reti 'Service Provider', identificarne i requisiti tecnici ed saper analizzare il funzionamento dei protocolli di routing utilizzati
- configurare i protocolli IGP (OSPF ed IS-IS) sia per il routing di IPv4 che per quello di IPv6
- configurare il protocollo BGP sia all'interno della rete ISP che nelle relazioni di Peering e di Transito
- definire e configurare le politiche di routing BGP per IPv4 ed IPv6
- fare troubleshooting in reti Service Provider

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider di medie/grandi dimensioni.
Progettisti di rete e responsabili di progetto per lo sviluppo di reti ISP
Candidati al conseguimento della certificazione Cisco CCNP Service Provider.

Prerequisiti

Conoscenza a livello introduttivo del routing IP. Conoscenza a livello intermedio della configurazione di apparati Cisco con IOS/IOS-XE ed IOS-XR. Le conoscenze necessarie sono conseguibili, ad esempio, con i corsi per le certificazioni CCNA o, preferibilmente, CCNA-Service Provider.



Il Routing IP nelle Reti ISP: aspetti avanzati

Il corso fornisce le competenze necessarie per configurare, verificare e risolvere i problemi relativi alla configurazione avanzata del BGP, del routing multicasting, per realizzare e gestire una rete Service Provider, sia con riferimento al trasporto del protocollo IPv4 che IPv6. La descrizione teorica degli argomenti trattati è completata da una rilevante attività *hands on* su un ricco laboratorio '*Carrier Class*', costituito da router Cisco con sistema operativo IOS e IOS-XR, che riproduce, in piccolo, architetture di rete Service Provider.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 642-883 "SPADVROUTE".

Agenda (5 giorni)





Connettività Clienti-ISP via BG:

- clienti Multi-Homed a un singolo ISP: utilizzo di route statiche
- clienti Multi-Homed a un singolo ISP: utilizzo solo di BGP
- clienti Multi-Homed a differenti ISP.

Il BGP nelle reti dei Service Provider:

- architettura di routing delle reti degli ISP
- Route Reflectors
- confederazioni BGP.

Aspetti di sicurezza:

- problemi e soluzioni
- contromisure
- Remote-Triggered Black-Hole Filtering (RTBH).

Meccanismi per la Stabilità:

- problemi e soluzioni
- Route Flap Damping
- SSO, NSF e NSR.

Controllo della velocità di convergenza:

- problemi e soluzioni
- Timer principali
- regolazione dei parametri delle connessioni TCP
- altre funzionalità.

Scalabilità della configurazione:

- BGP peer groups
- BGP peer templates
- BGP configuration templates.

Introduzione al Routing Multicast:

- Motivazioni e applicazioni
- principi generali
- indirizzi IPv4 Multicast.

Il protocollo IGMP:

- generalità
- IGMPv1 e IGMPv2
- IGMPv3 (cenni)
- Configurazione base.

Multicast negli switch:

- generalità
- IGMP snooping
- PIM snooping.

Protocolli di routing multicast:

- commutazione dei pacchetti multicast
- concetti generali
- alberi multicast
- protocolli dense-mode
- protocolli sparse-mode.

Il Routing IP nelle Reti ISP: aspetti avanzati

Il protocollo PIM:

- aspetti base
- PIM Sparse-Mode (PIM-SM)
- configurazione di PIM-SM.

Metodi per la selezione del RP:

- Auto-RP
- Bootstrap Router
- Anycast RP.

Modelli di servizio basati sul protocollo PIM:

- Source-Specific Multicast (SSM)
- PIM Bidirezionale (PIM-Bidir).

Routing Multicast Interdominio:

- scenario, problemi e soluzioni
- ruolo e configurazione del BGP
- il protocollo MSDP.

Multicast per IPv6:

- indirizzi IPv6 multicast
- protocollo Multicast Listener Discovery (MLD)
- PIM SM e SSM.

DNS e DHCP per IPv6:

- DNS per IPv6
- DHCPv6
- Prefix Delegation.

Supporto della QoS:

- supporto del modello DiffServ
- aspetti di configurazione.

«Utilities» per IPv6.

Integrazione e transizione IPv4-IPv6:

- scenari e modelli
- NAT64
- Tunneling in reti IPv4-only: tunneling static, 6to4 e 6rd.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- configurare il protocollo BGP in reti Service Provider relativamente alle sessioni con le reti cliente e nelle relazioni di *Peering* con altri sistemi autonomi
- descrivere ed utilizzare gli strumenti e le funzionalità disponibili per proteggere e ottimizzare il funzionamento del protocollo BGP in ambiente ISP
- introdurre in rete servizi IPv4 ed IPv6 multicast
- analizzare e configurare i meccanismi di transizione per introdurre IPv6 nelle reti ISP.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Cisco CCNP SP.

Prerequisiti

Conoscenza dei principi di base che governano il routing nelle reti 'Service Provider'.
Conoscenza di base della configurazione dei protocolli OSPF, IS-IS e BGP per IPv4 e per IPv6
Capacità operativa nella configurazione degli apparati Cisco basati su IOS, IOS-XE ed IOS-XR.
Tali competenze possono essere acquisite, ad esempio, con il corso 'Il Routing IP nelle Reti ISP' (IPN264).

Tecnologie dei backbone nelle reti ISP

Il corso descrive le modalità di impiego del 'Multiprotocol Label Switching' (MPLS) nel core delle reti Service Provider e le tecniche di ingegneria del traffico basate su MPLS (MPLS TE). Il corso tratta inoltre i meccanismi e le tecnologie utilizzati per fornire qualità del servizio (QoS) nelle reti ISP. La descrizione teorica degli argomenti trattati è completata da una rilevante attività hands on su un ricco laboratorio 'Carrier Class', costituito da router Cisco con sistema operativo IOS e IOS-XR, che riproduce, in piccolo, architetture di rete Service Provider.

Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 642-887 "SPCORE".

Agenda (5 giorni)





Introduzione a MPLS:
- motivazioni
- servizi MPLS.

Concetti fondamentali:
- componenti funzionali
- Label Switched Paths
- etichette.

Distribuzione delle associazioni <FEC, etichetta>:
- Label Distribution Protocol (LDP)
- LDP nei router Cisco
- distribuzione via BGP.

Convergenza di MPLS.

Implementazione di MPLS nell'IOS, IOS XE e IOS XR:
- prologo: Cisco Express Forwarding (CEF)
- configurazione base
- configurazione del protocollo LDP
- verifica e Troubleshooting.

MPLS nelle reti ISP:
- architettura di routing delle reti ISP
- architettura di routing BGP/MPLS
- sincronizzazione IGP-LDP.

Concetti fondamentali di MPLS Traffic Engineering:
- TE via MPLS
- costruzione del TE-LSDB
- determinazione dei percorsi
- segnalazione e gestione dei percorsi.

Implementazione di MPLS-TE nell'IOS, IOS XE e IOS XR:
- configurazioni base
- definizione di vincoli
- riottimizzazione dei Tunnel MPLS-TE
- verifica del funzionamento
- inoltro del traffico.

Protezione del traffico:
- modalità di protezione
- protezione dei collegamenti.

Aspetti avanzati di MPLS-TE nell'IOS, IOS XE e IOS XR:
- controllo automatico della banda
- Diffserv-aware TE.

Tecnologie dei backbone nelle reti ISP

Introduzione alla QoS IP:
- qualità del Servizio nelle Reti a Commutazione di Pacchetto
- indici di Qualità del Servizio
- fattori che influenzano la QoS e possibili soluzioni
- il modello Integrated Services (IntServ) : cenni.

Il modello Differentiated Services (DiffServ):
- architettura e Per Hop Behaviour (PHB).

Implementazione della QoS nell'IOS, IOS XE e IOS XR:
- Modular QoS CLI (MQC) e configurazioni base.

Classificazione e Colorazione del Traffico:
- Classificazione e Colorazione via MQC
- Classificazione e Colorazione via BGP (QPPB)
- Classificazione a Livello Applicativo (NBAR)
- Classificazione nei Tunnel VPN.

Gestione della banda:
- meccanismi di scheduling
- gestione della Banda nei router Cisco
- scheduling FIFO
- Class-Based Weighted Fair Queueing (CBWFQ)
- Low Latency Queueing (LLQ).

Gestione dei buffer:
- Weighted Random Early Detection (WRED)
- Explicit Congestion Notification (ECN).

Controllo del Traffico:
- meccanismi di controllo
- l'algoritmo Token Bucket
- Traffic Policing
- Local Packet Transport Service (LPTS)
- Traffic Shaping.

Supporto della QoS nelle reti IP/MPLS:
- gestione dei marker
- Tunnel DiffServ
- modelli di QoS nelle VPN.

Regole di Progettazione: Best Practice; classificazione e Politiche di QoS.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:
- comprendere i meccanismi di funzionamento di MPLS, i suoi vantaggi e le sue modalità di impiego nelle reti Service Provider
- analizzare e valutare i benefici del MPLS-Traffic Engineering per l'ottimizzazione dell'utilizzo delle risorse nel backbone delle reti ISP
- padroneggiare i meccanismi di QoS utilizzati nel backbone delle reti Service Provider
- pianificare, configurare, verificare e fare il troubleshooting delle funzionalità di cui sopra.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider di medie/grandi dimensioni. Candidati al conseguimento della certificazione Cisco CCNP Service Provider.

Prerequisiti

Conoscenza dei principi di base che governano il routing nelle reti 'Service Provider'. Conoscenza di base della configurazione dei protocolli OSPF, IS-IS e BGP per IPv4 e per IPv6.Capacità operativa nella configurazione degli apparati Cisco basati su IOS, IOS-XE ed IOS-XR. Tali competenze possono essere acquisite, ad esempio, con il corso 'Il Routing IP nelle Reti ISP' (IPN264).



Servizi VPN nelle reti ISP

Il corso fornisce le competenze necessarie alla pianificazione, configurazione e gestione di servizi VPN Layer 2 e Layer 3 in ambiente Service Provider. La descrizione teorica degli argomenti trattati è completata da una rilevante attività *hands on* su un ricco laboratorio '*Carrier Class*', costituito da router Cisco con sistema operativo IOS e IOS-XR, che riproduce, in piccolo, architetture di rete Service Provider.

Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 642-889 "SPEDGE".

Agenda (5 giorni)





Modelli di Reti Private Virtuali:

- Reti Private Fisiche e Virtuali
- modelli di comunicazione e topologie
- modello overlay
- modello peer-to-peer.

VPN IP BGP/MPLS : aspetti base:

- generalità
- piano di controllo
- piano dati
- configurazione di VPN any-to-any
- routing PE-CE (statico, RIPv2, EIGRP, OSPF, eBGP)
- Verifica e Troubleshooting.

VPN IP BGP/MPLS : aspetti avanzati:

- realizzazione di servizi VPN
- configurazioni fault-tolerant PE-CE
- connettività Internet
- servizi Carrier supporting Carriers (CsC)
- VPN Multiprovider.

Tunneling IPv6 in reti IPv4+MPLS:

- modello 6PE
- VPN IPv6 BGP/MPLS (6VPE).

VPN di Livello 2:

- motivazioni
- servizi e Modelli di L2VPN
- servizi Carrier Ethernet.

Il servizio VPWS (PW3):

- concetti fondamentali
- configurazioni Base
- trasporto di trame Ethernet
- servizi Any-to-Any.

Il servizio VPLS:

- concetti fondamentali
- piano di controllo
- configurazioni base
- VPLS gerarchiche (H-VPLS).

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- comprendere i meccanismi e le tecnologie utilizzati per realizzare Reti Private Virtuali (VPN) nell'ambiente di reti Service provider in tecnologia MPLS.
- pianificare, configurare e fare il troubleshooting di VPN Layer 3 e Layer 2 realizzate tramite MPLS in ambiente ISP.

Servizi VPN nelle reti ISP

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider di medie/grandi dimensioni.

Candidati al conseguimento della certificazione Cisco CCNP Service Provider.

Prerequisiti

Conoscenza dei principi di base che governano il routing nelle reti 'Service Provider'.

Conoscenza di base della configurazione dei protocolli OSPF, IS-IS e BGP per IPv4 e per IPv6

Capacità operativa nella configurazione degli apparati Cisco basati su IOS, IOS-XE ed IOS-XR.

Conoscenza di MPLS e della sua configurazione.

Tali competenze possono essere acquisite, ad esempio, con i corsi 'Il Routing IP nelle Reti ISP' (IPN264) e Tecnologie dei backbone nelle reti ISP' (IPN266).



Next Generation Multicast VPN

Il primo modello di servizi Multicast VPN, supportato da Cisco, ma implementato anche nei router Juniper, è il modello basato sul «draft-rosen-vpn-mcast», anche noto come *Draft-Rosen*.
Benché oggi sia classificato come *historical*, è ancora implementato. L'idea alla base del modello *Draft-Rosen* è intuitiva: rendere il backbone IP/MPLS, agli occhi dei router CE, simile ad una LAN.
Il modello *Draft-Rosen,* non utilizzando il BGP nel piano di controllo né MPLS sul piano dati, si è però dimostrato poco scalabile e soprattutto non conforme al modello generale di VPN BGP/MPLS. Per questo motivo è stato sviluppato un nuovo modello NG-MVPN, (*Next Generation*-MVPN), che si integra perfettamente con il modello di VPN unicast BGP/MPLS. Il nuovo modello, supportato soprattutto da Juniper, utilizza il BGP nel piano di controllo, mentre sul piano dati può utilizzare varie alternative, tra cui LSP MPLS P2MP realizzati via RSVP-TE o mLDP.
Il modello NG-MPVN è uno standard definito dalle due RFC:

- RFC 6513 «Multicast in MPLS/BGP IP VPNs», Febbraio 2012.
- RFC 6514 «BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs», Febbraio 2012.

Il corso illustra gli aspetti principali del nuovo modello, il funzionamento, e gli aspetti di configurazione. È prevista una rilevante attività di laboratorio *hands on,* costituito da router Juniper interconnessi con router Cisco.

Agenda (2 giorni)



Aspetti propedeutici:

- richiami sui fondamenti del routing multicast e del protocollo PIM
- LSP MPLS point-to-multipoint via RSVP-TE e mLDP
- cenni sul modello draft-rosen.

Next-Generation MVPN:

- piano di controllo: ruolo del BGP, tipi di NLRI e nuovi attributi
- inclusive tree e selective tree
- opzioni per il piano dati.

Configurazioni in ambiente JUNOS:

- aspetti base
- routing PE-CE via PIM SSM
- routing PE-CE via PIM SM
- configurazione di selective trees.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- comprendere gli aspetti fondamentali del modello NG-MVPN
- comprendere il funzionamento del piano di controllo e in particolare del ruolo del BGP
- valutare e utilizzare le alternative disponibili per il piano dati
- configurare un servizio NG-MVPN in ambiente JUNOS.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti service provider e reti enterprise di grandi dimensioni.

Prerequisiti

È richiesta una conoscenza generale dei servizi L3VPN BGP/MPLS e delle basi del routing multicast, incluso il protocollo PIM. Inoltre, per massimizzare l'utilità delle esercitazioni di laboratorio, è bene avere conoscenze sui temi trattati nei corsi "Introduzione alla Configurazione di Router Juniper" (INP252) e "MPLS nel JUNOS Juniper" (IPN 258).



MPLS: dalla Teoria alla Pratica

Il corso introduce gli aspetti fondamentali di MPLS, i paradigmi su cui si basa, la sua integrazione con le reti di livello 2 e i principali servizi supportati, focalizzando l'attenzione sui vantaggi che la sua introduzione in rete comporta. Oltre alle sessioni teoriche, è prevista una consistente parte pratica di configurazione in ambiente IOS Cisco e/o JUNOS Juniper di router MPLS,e simulazioni in laboratorio di backbone MPLS e relativi servizi offerti. Saranno presentati anche dei Case Studies di configurazioni su router in produzione.
Il corso è nei percorsi di certificazione Cisco CCNP-SP e Juniper JNCIS-SP, JNCIP-SP.

Agenda (3 giorni)





L'evoluzione del trasporto IP nei grandi Backbone IP.

Multi Protocol Label Switching (MPLS):

- concetti fondamentali
- distribuzione delle etichette
- trasporto di MPLS su livello 2
- architettura di routing BGP/MPLS
- esercitazioni di laboratorio: configurazioni di MPLS nell'IOS Cisco e nel JUNOS Juniper.

BGP/MPLS Virtual Private Networks (VPNs):

- concetti fondamentali: modello peer-to-peer, VRF, Route Distinguisher e Route Target, MP-BGP, MPLS
- routing PE-CE: routing statico, eBGP
- realizzazione di servizi VPN nell'IOS Cisco e nel JUNOS Juniper
- intranet, extranet e altre topologie
- cenni sulle modalità di accesso a Internet da siti VPN
- esercitazioni di laboratorio: configurazioni di VPN any-to-any nell'IOS Cisco e nel JUNOS Juniper.

Traffic Engineering (TE):

- TE nelle reti IP/MPLS
- cenni al protocollo di segnalazione RSVP-TE
- applicazioni alla protezione del traffico (Fast ReRouting)
- aspetti di configurazione e troubleshooting
- esercitazioni di laboratorio: realizzazione di ER-LSP e tunnel di backup via MPLS-TE nell'IOS Cisco e nel JUNOS Juniper.

Obiettivi

Al termine del corso i partecipanti:

- apprenderanno i fondamenti dello standard MPLS
- conosceranno i principali servizi che è possibile offrire tramite MPLS
- avranno acquisito gli elementi per valutare i vantaggi dell'introduzione di MPLS nelle reti IP
- conosceranno il funzionamento e la realizzazione di VPN di Livello 3
- saranno in grado di effettuare configurazioni di base dei servizi MPLS in reti Cisco e/o Juniper.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Conoscenza delle reti IP e esperienza di base di configurazione dei router Cisco e/o Juniper per ciò che riguarda: indirizzi IP, protocolli di routing, liste di accesso standard nell'IOS Cisco e routing policy nel JUNOS Juniper.

MPLS: servizi avanzati

Il corso, dopo brevi richiami sullo standard e sui principali servizi MPLS, ha l'obiettivo di introdurre alcuni nuovi e interessanti aspetti di MPLS quali: il trasporto delle trame L2, con particolare riferimento a Ethernet over MPLS, alcuni servizi VPN avanzati come CsC e VPN Multi-Provider, nuove funzionalità del Traffic Engineering come i backup auto-tunnels, e infine il trasporto di IPv6 su reti IP/MPLS. Oltre alle sessioni teoriche, è prevista una consistente parte pratica di configurazione in ambiente IOS Cisco e/o JUNOS Juniper di servizi MPLS.

Il corso rientra nei percorsi di certificazione Cisco CCIE Service Provider e Juniper JNCIE-SP.

Agenda (3 giorni)





Multi Protocol Label Switching (MPLS):

- richiami sui concetti fondamentali
- distribuzione delle etichette
- architettura di routing BGP/MPLS
- BGP/MPLS Virtual Private Networks (VPNs).

Servizi avanzati delle VPN BGP/MPLS:

- servizio Carrier Supporting Carriers (CsC)
- VPN Multi-provider
- esercitazioni di laboratorio: configurazione di servizi CsC e VPN Multi-provider nell'IOS Cisco e nel JUNOS Juniper.

Servizi avanzati di Traffic Engineering (TE):

- richiami sul Traffic Engineering MPLS
- Facility Backup e One-to-one Backup
- Backup Auto-Tunnels
- esercitazioni di laboratorio: configurazione di tunnel MPLS-TE nell'IOS Cisco e nel JUNOS Juniper.

VPN di Livello 2 (L2VPN):

- servizi L2VPN
- il servizio Virtual Private Wire Service (VPWS)
- trasporto di Ethernet e ATM su reti IP/MPLS
- il servizio VPLS (cenni)
- esercitazioni di laboratorio: configurazione di pseudo-wire nell'IOS Cisco e nel JUNOS Juniper.

Trasporto di pacchetti IPv6 su reti IP/MPLS:

- il modello 6PE
- trasporto di pacchetti iPv6 nelle VPN BGP/MPLS: il modello 6VPE.
- esercitazioni di laboratorio: configurazione del modello 6PE nell'IOS Cisco e nel JUNOS Juniper.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- i servizi avanzati realizzabili tramite il modello di VPN BGP/MPLS (topologie particolari, servizi CsC, VPN multi-provider)
- i servizi avanzati realizzabili tramite il Traffic Engineering MPLS
- i concetti base per la realizzazione di servizi L2VPN (VPWS, VPLS)
- l'utilizzo di MPLS nella migrazione IPv4-IPv6.

Destinatari

Amministratori e tecnici di rete (end-user, internet service provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti ip in ambiente enterprise e isp.

Prerequisiti

Conoscenza delle reti IP e esperienza di base di configurazione dei router Cisco e/o Juniper, per ciò che riguarda indirizzi IP, protocolli di routing (OSPF, BGP), liste di accesso standard nell'IOS Cisco e routing policy nel JUNOS Juniper. Conoscenza di base dello standard MPLS e dei servizi MPLS come VPN e Traffic Engineering (temi trattati nel corso IPN272).

MPLS nell'IOS XR Cisco

Il corso fornisce le competenze operative sulla configurazione base ed avanzata di MPLS negli apparati Cisco *carrier-grade*, che utilizzano il sistema operativo IOS XR. Saranno trattati, oltre ai concetti e protocolli fondamentali di MPLS, tutti i principali servizi MPLS, come ad esempio, *Traffic Engineering*, *Fast ReRouting*, L3VPN e L2VPN. È prevista una rilevante attività di laboratorio *hands on,* costituito da router Cisco basati su IOS XR e IOS.

Agenda (3 giorni)



Richiami sui concetti fondamentali di MPLS:

- componenti funzionali
- Etichette e Label Switched Path
- protocolli per la Distribuzione delle etichette: LDP, RSVP-TE, BGP.

Implementazione base di MPLS nell'IOS XR:

- configurazione base; configurazione del protocollo LDP
- verifica e troubleshooting.

Concetti fondamentali di MPLS *Traffic Engineering:*

- costruzione del TE-LSDB
- determinazione dei percorsi
- segnalazione e gestione dei percorsi
- servizi MPLS-TE : *Fast ReRouting* (FRR).

Implementazione di MPLS-TE nell'IOS XR:

- configurazioni base
- definizione di vincoli
- riottimizzazione dei Tunnel MPLS-TE
- verifica del funzionamento
- inoltro del traffico
- configurazione del FRR.

Richiami sulle Reti Private Virtuali IP BGP/MPLS (L3VPN).

Implementazione di servizi L3VPN nell'IOS XR:

- configurazione di VPN *any-to-any*
- Routing PE-CE; verifica e troubleshooting.

Servizi L2VPN: VPWS e VPLS.

Il servizio Virtual Private Wire Service (VPWS):

- concetti fondamentali
- EoMPLS (Ethernet over MPLS)
- configurazione di servizi VPWS nell'IOS XR.

Il servizio Virtual Private LAN Service (VPLS):

- funzioni e protocolli del piano di controllo; piano dati
- implementazione del servizio VPLS nell'IOS XR.

Obiettivi

Al termine del corso i partecipanti saranno in grado di configurare in ambiente IOS XR, gli aspetti base ed avanzati di MPLS, i tunnel MPLS-TE e i servizi di Fast ReRouting, e i servizi basati sull'architettura di routing BGP/MPLS (L3VPN e L2VPN).

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider e Enterprise di medie/grandi dimensioni. Progettisti, system engineer, personale di supporto tecnico che hanno bisogno di conoscere le caratteristiche e la configurazione dei router Cisco con IOS-XR.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze sui temi trattati nel corso "MPLS: dalla Teoria alla Pratica" (INP272).



Networking IP in ambiente Huawei

Il corso offre una panoramica introduttiva sui meccanismi di switching e di routing, descrivendo le principali tecnologie di livello 2 e 3, con riferimento, in particolare, ad apparati Huawei. Fornisce, inoltre, le competenze di base e la conoscenza del sistema operativo 'Versatile Routing Platform' (VRP) necessarie alla configurazione di apparati Huawei in ambiente LAN e WAN. È prevista una rilevante attività di laboratorio 'hands on' su apparati Huawei.
Il corso permette di acquisire le competenze necessarie per sostenere l'esame di certificazione Huawei HC-211-ENU "Huawei Certified Datacom Associated" (HCDA).

Agenda (8 giorni)





Principi di comunicazione dati:

- architetture e protocolli di comunicazione
- reti per dati a circuito e a pacchetto
- principi di comunicazione dati e modelli stratificati
- il modello di riferimento ISO/OSI
- servizi Connectionless e Connection-Oriented
- architetture di rete per dati WAN.

Architettura TCP/IP:

- internetworking e architettura TCP/IP
- Internet Protocol (IP): funzionalità di IP ed indirizzamento
- conversione degli indirizzi IP in indirizzi fisici (ARP)
- Internet Control Message Protocol (ICMP)
- protocolli di livello trasporto: UDP e TCP
- il Dynamic Host Configuration Protocol (DHCP)
- indirizzamento privato e Network Address Translation (NAT)
- I principali Applicativi su reti IP.
- esercitazione teorica: costruzione di un piano di indirizzamento IP con VLSM.

Introduzione alle famiglie di apparati Huawei ed al sistema operativo Huawei VRP:

- le famiglie di router e di switch Huawei e le loro funzionalità
- architettura del VRP: General Control Plane, Service Control Plane, System Service Plane, System Management Plane e Data Plane
- introduzione alla Command Line Interface fornita dal VRP.
- accesso tramite console, telnet ed ssh
- utenti e privilegi e le 'Command View'
- gestione dei file e delle configurazioni
- configurazioni di base: indirizzi, accesso telnet, utenti e privilegi
- strumenti di base per il troubleshooting di rete in ambiente Huawei: ping, traceroute, lldp, telnet, ssh
- laboratorio Hands-on: Configurazione di base di router Huawei; analisi e troubleshooting di base.

Architetture di rete locale (LAN):

- reti LAN: mezzi trasmissivi, topologie e protocolli di accesso
- il modello IEEE 802: livello fisico, MAC ed LLC
- il protocollo IEEE 802.3
- evoluzione di Ethernet: da 10 Mbit/s a 100Gbit/s
- i protocolli Spanning Tree e Rapid Spanning Tree
- cenni sul Multiple Spanniung Tree (MST)
- introduzione su Bridging e Switching
- domini di collisione; learning e filtraggio delle trame
- tabelle degli indirizzi MAC (CAM)
- virtual LAN e trunking.
- laboratorio Hands-on: Configurazione e troubleshooting di Switch, VLAN e Spanning Tree.

Introduzione al routing IP:

- funzionalità di routing e forwarding; Tabelle di routing; Routing statico e dinamico
- intervlan routing: 'Router on a stick' e Multilayer switching
- configurazione di rotte statiche su VRP
- laboratorio Hands-on: Configurazione e troubleshooting di InterVLAN Routing e routing statico.

Networking IP in ambiente Huawei

Ridondanza del Default Gateway (First Hop Redundancy – FHR):
- come ridondare l'accesso al default gateway o ad altre rotte statiche
- introduzione ai protocolli FHRP
- il protocollo Virtual Router Redundancy Protocol (VRRP)
- configurazione di VRRP su router Huawei
- laboratorio Hands-on: Configurazione di VRRP.

Protocolli di routing IP:
- routing interno ed esterno
- protocolli di routing Distance Vector e Link State
- distanza amministrativa, metrica, convergenza
- il protocollo RIP ed il RIPv2.
- il protocollo OSPF: introduzione, adiacenze, suddivisione in aree, configurazione
- laboratorio Hands-on: Configurazione e troubleshooting di routing dinamico con OSPF in ambiente singola area e multiarea.

Sicurezza su router Huawei:
- funzionalità e tipologie di firewall
- filtraggio del traffico tramite Access Control List (ACL)
- configurazione di ACL su router Huawei
- laboratorio Hands-on: Configurazione di ACL.

Tecnologie e protocolli per reti geografiche (WAN):
- connessioni seriali punto-punto: protocolli HDLC e PPP
- configurazione del PPP sui router.
- implementazione e configurazione di HDLC e PPP sui router Huawei
- il protocollo e le reti Frame-Relay
- tipi di LMI ed Incapsulamento
- laboratorio Hands-on: Configurazione di Frame Relay tra sito centrale e siti periferici.

Indirizzamento privato e NAT
- terminologia; NAT statico e dinamico; NAT Overloading; configurazione del NAT
- laboratorio Hands-on: Configurazione di NAT.

Introduzione ad IPv6:
- caratteristiche generali e differenze rispetto ad IPv4
- introduzione ai protocolli di routing per IPv6 ed alla loro configurazione su router Cisco
- cenni sui principali meccanismi di transizione.
- configurazioni di base di IPv6 su router Huawei
- laboratorio Hands-on: Configurazione di IPv6 con VRP.

Obiettivi

Comprendere la struttura ed i meccanismi base di funzionamento dei protocolli dell'architettura TCP/IP.
Comprendere la struttura ed i meccanismi base di funzionamento di reti IP in ambiente LAN e WAN.
Saper Utilizzare i comandi di base del sistema operativo Huawei VRP.
Saper configurare, gestire ed effettuare il troubleshooting di reti Huawei in ambito LAN e WAN di piccole e medie dimensioni.
Acquisire conoscenze di base sul protocollo IPv6 e sulla sua configurazione su router Huawei.
Prepararsi per la certificazione HCDA.

Destinatari

Tecnici di rete ed operatori di help desk che operino nel settore del networking, o ad altre figure professionali che abbiano bisogno di acquisire competenze introduttive di buon livello sulla configurazione e la gestione di router e switch Huawei.
Chiunque sia interessato a conseguire la certificazione Huawei HCDA.

Prerequisiti

Conoscenze di base sulle reti e sull'utilizzo di Personal Computer.



Networking IP in ambiente Huawei - Fast Track

Il corso offre una panoramica introduttiva sui meccanismi di switching e di routing, descrivendo le principali tecnologie di livello 2 e 3, con riferimento, in particolare, ad apparati Huawei. Fornisce, inoltre, le competenze di base e la conoscenza del sistema operativo 'Versatile Routing Platform' (VRP) necessarie alla configurazione di apparati Huawei in ambiente LAN e WAN. È prevista una rilevante attività di laboratorio 'hands on' su apparati Huawei.
Il corso permette di acquisire le competenze necessarie per sostenere l'esame di certificazione Huawei HC-211-ENU "Huawei Certified Datacom Associated" (HCDA).

Agenda (4 giorni)





Introduzione alle famiglie di apparati Huawei ed al sistema operativo Huawei VRP:

- le famiglie di router e di switch Huawei e le loro funzionalità
- architettura del VRP: General Control Plane, Service Control Plane, System Service Plane, System Management Plane e Data Plane
- introduzione alla Command Line Interface fornita dal VRP.
- accesso tramite console, telnet ed ssh
- utenti e priviliegi
- le 'Command View'
- gestione dei file e delle configurazioni
- configurazioni di base: indirizzi, accesso telnet, utenti e privilegi
- strumenti di base per il troubleshooting di rete in ambiente Huawei: ping, traceroute, lldp, telnet, ssh
- laboratorio Hands-on: Configurazione di base di router Huawei; analisi e troubleshooting di base.

Architetture di rete locale (LAN):

- richiami sui protocolli di Spanning Tree e Rapid Spanning Tree
- cenni sul Multiple Spanniung Tree (MST)
- richiami su Bridging e Switching
- tabelle degli indirizzi MAC (CAM)
- Virtual LAN e trunking.
- laboratorio Hands-on: Configurazione e troubleshooting di Switch, VLAN e Spanning Tree.

Richiami sul routing IP:

- funzionalità di routing e forwarding; Tabelle di routing; Routing statico e dinamico
- InterVLAN routing: 'Router on a stick' e Multilayer switching
- configurazione di rotte statiche su VRP
- laboratorio Hands-on: Configurazione e troubleshooting di InterVLAN Routing e routing statico.

Ridondanza del Default Gateway (First Hop Redundancy – FHR):

- come ridondare l'accesso al default gateway o ad altre rotte statiche
- introduzione ai protocolli FHRP
- il protocollo Virtual Router Redundancy Protocol (VRRP)
- configurazione di VRRP su router Huawei
- laboratorio Hands-on: Configurazione di VRRP.

Protocolli di routing IP:

- routing interno ed esterno
- protocolli di routing Distance Vector e Link State
- distanza amministrativa, metrica, convergenza
- il protocollo RIP ed il RIPv2.
- il protocollo OSPF: introduzione, adiacenze, suddivisione in aree, configurazione.

Laboratorio Hands-on:

- configurazione e troubleshooting di routing dinamico con OSPF in ambiente singola area e multiarea.

Sicurezza su router Huawei:

- funzionalità e tipologie di firewall
- filtraggio del traffico tramite Access Control List (ACL)
- configurazione di ACL su router Huawei
- laboratorio Hands-on: Configurazione di ACL.

Networking IP in ambiente Huawei - Fast Track

Tecnologie e protocolli per reti geografiche (WAN):

- connessioni seriali punto-punto: protocolli HDLC e PPP
- configurazione del PPP sui router.
- implementazione e configurazione di HDLC e PPP sui router Huawei
- il protocollo e le reti Frame-Relay
- tipi di LMI ed Incapsulamento
- laboratorio Hands-on: Configurazione di Frame Relay tra sito centrale e siti periferici.

Indirizzamento privato e NAT

- terminologia
- NAT statico e dinamico
- NAT Overloading
- configurazione del NAT
- laboratorio Hands-on: Configurazione di NAT.

Introduzione ad IPv6:

- caratteristiche generali e differenze rispetto ad IPv4
- introduzione ai protocolli di routing per IPv6 ed alla loro configurazione su router Cisco
- cenni sui principali meccanismi di transizione
- configurazioni di base di IPv6 su router Huawei
- laboratorio Hands-on: Configurazione di IPv6 con VRP.

Obiettivi

Saper Utilizzare i comandi di base del sistema operativo Huawei VRP.
Saper configurare, gestire ed effettuare il troubleshooting di reti Huawei in ambito LAN e WAN di piccole e medie dimensioni.
Acquisire conoscenze di base sul protocollo IPv6 e sulla sua configurazione su router Huawei.
Prepararsi per la certificazione HCDA.

Destinatari

Tecnici di rete ed operatori di help desk che operino nel settore del networking, o ad altre figure professionali che abbiano bisogno di acquisire competenze introduttive di buon livello sulla configurazione e la gestione di router e switch Huawei.
Chiunque sia interessato a conseguire la certificazione Huawei HCDA.

Prerequisiti

Buona conoscenza del modello OSI, dell’architettura TCP/IP, del funzionamento delle LAN.
Conoscenza introduttiva del routing IP.
Una versione ‘Fast Track’ per la preparazione alla certificazione HCDA è consigliata per chi è già in possesso di certificazione analoga di altri costruttori, come ad esempio CCNA Routing & Switching (Cisco) oppure JNCIA-Junos (Juniper).



Enterprise Routing in tecnologia Huawei

Il corso tratta il tema generale del Routing IP, descrivendo i principali protocolli di routing utilizzati nelle reti Enterprise di medie e grandi dimensioni, per il trasporto sia di IP versione 4 che di IP versione 6. Dopo una descrizione introduttiva della nuova versione del protocollo IP (IPv6), il corso presenta una descrizione generale dell'architettura logica di Internet, i modelli di routing Intra-AS ed Inter-AS e le principali caratteristiche dei protocolli di routing Distance Vector e Link State. Si passa quindi ad una descrizione più approfondita dei protocolli di routing più utilizzati nelle reti Enterprise, sia in ambiente intra-dominio (OSPF) che inter-dominio (BGP). Sono poi analizzate nel dettaglio le problematiche di redistribuzione tra protocolli di routing e di filtraggio degli annunci ed i meccanismi di routing multicast.
Per ciascuno degli argomenti trattati viene fatto parimenti riferimento sia alle implementazioni relative ad IPv4 che ad IPv6. La descrizione teorica degli argomenti trattati è completata da una rilevante attività *hands on* su un ricco laboratorio, costituito da router Huawei che riproduce situazioni analoghe a quelle reali.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Huawei HC-221 "Implementing Enterprise Routing Network (HCNP-R&S-IERN)", parte del percorso di certificazione "Huawei Certified Network Professional" (HCNP).

Agenda (5 giorni)





L'architettura di Internet:

- Gli organismi di governo di standardizzazione
- Gli Autonomous Systems (AS)
- Provider di servizi Internet (ISP), Peering e Transit, Provider Tier-1 e Tier-2, IXP.

Introduzione ad IP versione 6:

- Struttura degli indirizzi
- Indirizzi Link Local, Global e Unique Local
- ICMPv6 e StateLess Address Auto Configuration (SLAAC)
- Cenni sui principali meccanismi di transizione.

Principi di routing:

- Routing Intra-Dominio ed Inter-Dominio
- Caratteristiche generali dei protocolli (metrica, grado di preferenza, tabelle di routing)
- Protocolli di routing Distance Vector (DV) e Link State (LS).

Il protocollo OSPF:

- Richiami sull'impiego di OSPF in area singola
- Tipi di router, LSA, aree
- Configurazione di OSPF multiarea su VRP Huawei
- Aspetti avanzati di OSPF: aggregazione, virtual-link, sicurezza, OSPF su reti NBMA
- OSPFv3 per IPv6.

Routing inter-dominio: il protocollo BGP:

- Funzionamento di base, sessioni e attributi BGP, processo di selezione
- Implementazione di base del BGP nel VRP Huawei
- Filtraggio degli annunci: filtri inbound/outbound, tool per la selezione delle rotte
- Politiche di routing: il processo di selezione nei router Huawei, gestione del traffico outbound e inbound.
- Route Reflector e Confederation
- Utilizzo del Multiprotocol BGP per IPv6.

Meccanismi di Path Control: redistribuzione, filtraggio, distanza amministrativa, Policy Based Routing.

Routing Multicast:

- Principi generali di funzionamento di IP multicast
- Multicast host-to-router e protocollo IGMP
- Protocolli di routing multicast: PIM-DM e PIM-SM
- PIM-SM: meccanismi di selezione del Rendezvous Point
- Multicast in IPv6 e differenze rispetto ad IPv4.

Enterprise Routing in tecnologia Huawei

Obiettivi

Al termine del corso i partecipanti:

- conosceranno i meccanismi di funzionamento dei protocolli di routing IP e la loro interazione nelle reti
- conosceranno l'implementazione in ambiente Huawei dei protocolli intra-dominio (OSPF), e inter-dominio (BGP)
- sapranno progettare e effettuare configurazioni di scenari complessi di rete.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti enterprise di medie e grandi dimensioni.

Prerequisiti

Conoscenza dell'architettura TCP/IP. Capacità operativa su apparati Huawei a livello introduttivo. Sono inoltre utili competenze operative nella configurazione di apparati di routing di qualsiasi vendor.



Enterprise Switching in tecnologia Huawei

Il corso descrive nel dettaglio le tecnologie di Switching impiegate nelle reti locali e metropolitane di medie e grandi dimensioni. Nella trattazione si fa principalmente riferimento alla progettazione, installazione ed amministrazione di Reti di Campus e reti Metro-Ethernet con l'impiego di tecnologie di switching multilayer Huawei.
Ad integrazione della trattazione teorica, il corso prevede una rilevante attività 'hands on' su un ricco laboratorio, costituito da switch Huawei L2 e multilayer, che riproduce una rete di campus di grandi dimensioni.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Huawei HC-222 "Implementing Enterprise Switching Network (HCNP-R&S-IESN)", parte del percorso di certificazione "Huawei Certified Network Professional" (HCNP).

Agenda (5 giorni)





Overview sulle reti di Campus:

- la struttura di una rete di campus ed il modello gerarchico: livelli di accesso, distribuzione e "core"
- architettura di reti di campus di piccole, medie e grandi dimensioni.

Introduzione alle Virtual LAN:

- tipi di link: access, trunk e ibridi
- metodi per l'attribuzione della membership alle porte
- il protocollo 802.1q.
- routing tra le VLAN.

Il protocollo dello Spanning Tree:

- richiami sullo STP, spanning tree singolo e "Per VLAN Spanning Tree"
- Rapid Spanning Tree Protocol (RSTP)
- Mutiple Spanning Tree Instance (MSTI) standard 802.1s.

Funzionalità di sicurezza nelle reti switched:

- tipi di attacchi di livello 2 (MAC Flooding, DHCP Spoofing, VLAN Hopping, etc.)
- Introduzione al protocollo DHCP ed alla sua configurazione
- Meccanismi di protezione: DHCP snooping, Dynamic ARP inspection
- Port Security e IEEE 802.x
- VLAN ACL e Private VLAN.

Introduzione alle reti metro Ethernet:

- architettura di una rete Metro Ethernet
- Ethernet su SDH e Ethernet su WDM
- interconnessione con Switch Layer 2 e 3
- utilizzo delle VLAN nelle Metro Ethernet: Stacked VLAN e incapsulation QinQ

MPLS e suo utilizzo nelle reti metroethernet:

- Introduzione ad MPLS
- Il protocollo LDP
- Cenni sulle VPN L2 in MPLS.

Enterprise Switching in tecnologia Huawei

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- scegliere l'architettura di rete più idonea per reti locali e di campus, anche di grandi dimensioni
- configurare switch Cisco di livello 2 e livello 3 anche in architetture di rete complesse
- svolgere attività di troubleshooting su reti LAN, di Campus e in area metropolitana
- mettere in sicurezza gli apparati di rete e configurare i meccanismi di sicurezza di livello 2.

Destinatari

Il corso è rivolto a tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti enterprise di medie e grandi dimensioni.

Prerequisiti

Conoscenza generale delle reti IP e delle architetture di reti LAN. Capacità operative di base nella configurazione di apparati Huawei.



Sicurezza, Alta Affidabilità e QoS in Tecnologia Huawei

Il corso tratta alcuni temi, di grande rilevanza, che completano la panoramica tecnologica sulle reti Enterprise in ambiente Huawei: sicurezza, alta affidabilità e qualità del servizio.
Ad integrazione della trattazione teorica, il corso prevede una rilevante attività 'hands on' su un ricco laboratorio, costituito da apparati di rete Huawei.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Huawei HC-223 "Improving Enterprise Network Performance (HCNP-R&S-IENP)", parte del percorso di certificazione "Huawei Certified Network Professional" (HCNP).

Agenda (5 giorni)





Introduzione ala sicurezza nelle reti Enterprise:

- introduzione ai meccanismi di sicurezza in tecnologia Huawei
- liste di accesso e Firewall
- lo 'zoning'
- modalità operative di un firewall: route, transparent, composite
- Application Specific Packet Filter (ASPF)
- Blacklisting e Port Mapping
- Intrusion Detection Systems e sua interazione col Firewall
- VPN e Virtual Firewall
- configurazione di base dei firewall Huawei UGS.

Il Network Address Translation (NAT):

- principi di funzionamento
- il NAT nella sicurezza di rete: NAT + ALG + ASPF
- istanze multiple di NAT
- configurazione.

Tipi di attacchi e relative tecniche di difesa:

- attacchi DOS
- attacchi basati su snooping
- attacchi con pacchetti 'defective'.

Virtual Router Redundancy Protocol (VRRP)

- motivazioni
- principi di funzionamento
- macchina a stati
- Tracking
- Configurazione.

Meccanismi per Alta Affidabilità (High Availability):

- Non Stop Forwarding (NSF) e Gracefull Restarting (GR)
- Bidirectional Forwarding Detection (BFD).

Meccanismi di qualità del servizio (QoS):

- Overview sui parametri di QoS nelle reti IP
- modelli di QoS: Integrated Services (IS) e Differenziated Services (DS)
- Classification e Marking
- Policing e shaping
- meccanismi di scheduling e gestione delle code
- miglioramento dell'efficienza dei link
- configurazione.

Sicurezza, Alta Affidabilità e QoS in Tecnologia Huawei

Obiettivi

Al termine del corso i partecipanti saranno in grado di scegliere le tecnologie Huawei più idonee, progettare le soluzioni più adatte, ed effettuare le configurazioni degli apparati per:

- mettere in sicurezza una rete Enterprise utilizzando firewall USG
- massimizzare la disponibilità della rete
- mettere in campo le necessarie funzionalità di QoS.

Destinatari

Il corso è rivolto a tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti enterprise di medie e grandi dimensioni.

Prerequisiti

Conoscenza generale delle reti IP e delle architetture di reti LAN. Capacità operative di base nella configurazione di apparati Huawei.



Soluzioni di Wan Governance: IPANEMA

La rete WAN rappresenta uno dei pilastri del business aziendale. La tecnologia IPANEMA permette, attraverso la sua sonda ip|engine, di avere la piena visibilità del traffico che attraversa la rete e di determinare le performance (bandwidth, jitter, delay) delle applicazioni. Le funzionalità di ottimizzazione e compressione garantiscono un miglioramento dei livelli di servizio delle applicazioni "business oriented".
Gli argomenti illustrati durante il corso saranno affiancati da attività di laboratorio durante le quali i partecipanti avranno modo di mettere in pratica quanto appreso.

Agenda (2 giorni)



Concetti e componenti del sistema IPANEMA.

Architettura.

Visibility.

Ottimizzazione.

Domain Management.

Configurazione ip|boss.

Compressione.

Accelerazione.

Report (ip|reporter).

Obiettivi

A conclusione del corso i partecipanti avranno acquisito le conoscenze necessarie per il design, la configurazione e il troubleshooting della tecnologia IPANEMA.

Destinatari

Il corso è rivolto ai responsabili dei sistemi informativi, progettisti e amministratori di sistemi di rete.

Prerequisiti

Conoscenza di base dei Sistemi Informativi, TCP/IP.

IPV6 e gli scenari di migrazione

Il corso fornisce una descrizione generale del protocollo IPv6 evidenziandone le principali differenze rispetto a IPv4. Sono descritti gli scenari di introduzione di IPv6 in rete ed i meccanismi attualmente previsti per consentire la coesistenza dei due protocolli.

Agenda (1 giorno)

Introduzione:

- limitazioni di IPv4 e motivazioni per il passaggio ad IPv6
- principali caratteristiche di IPv6.

Il protocollo IP versione 6:

- formato dell'intestazione e Next-headers
- spazio di indirizzamento unicast, multicast e anycast
- prefissi IPv6 e loro allocazione
- indirizzi global, link local, unique local, multicast
- esempi di pianificazione dell'indirizzamento IPv6: rete Enterprise e rete ISP.

Il protocollo ICMPv6:

- Neighbor & Router discovery
- diagnostica e Address Autoconfiguration
- cenni sulla configurazione di IPv6 sugli host.

Introduzione al Routing in IPv6:

- RIPng
- EIGRPv6
- Estensioni per IS-IS
- BGP per IPv6
- OSPFv3.

Meccanismi di transizione verso IPv6:

- Dual Stack
- Tunnelling statico ed automatico
- meccanismi NAT-based (DS-lite, NAT64)
- meccanismo 6to4
- modello 6PE.

Obiettivi

Al termine del corso i partecipanti sapranno:

- analizzare le motivazioni per il passaggio al protocollo IPv6
- comprendere i principali meccanismi di funzionamento di IPv6 e le differenze con IPv4
- valutare i meccanismi di transizione da IPv4 ad IPv6 e di convivenza dei due protocolli.

Destinatari

Direttori e Responsabili ICT, Amministratori di rete e tecnici di rete e Data Center e tutti coloro che vogliano comprendere le esigenze di migrazione e i principi base del nuovo protocollo.

Prerequisiti

Conoscenza generale dell'architettura di comunicazione TCP/IP e dell'indirizzamento IP.

IPv6: istruzioni per l'uso

Il corso fornisce una descrizione approfondita del protocollo IPv6 e dei protocolli ad esso associati. Sono inoltre descritti i meccanismi che verranno utilizzati per consentire la migrazione e la coesistenza tra IPv4 ed IPv6. Le attività didattiche teoriche sono affiancate da una consistente attività pratica di configurazione effettuata sui laboratori IPv6 di Reiss Romoli.

Agenda (4 giorni)



Introduzione:

- limitazioni di IPv4 e motivazioni per il passaggio ad IPv6
- principali caratteristiche di IPv6
- politiche di allocazione degli indirizzi IPv6: ICANN, RIR e LIR
- politiche RIPE di allocazione degli indirizzi IPv6
- rapporti con RIPE e Richiesta dei prefissi IPv6.

Il protocollo IP versione 6:

- formato dell'intestazione e Next-headers
- spazio di indirizzamento unicast, multicast e anycast
- prefissi IPv6 e loro allocazione
- indirizzi global, link local, unique local, multicast.
- piano di indirizzamento della rete in Ipv6
- Esempi di pianificazione dell'indirizzamento IPv6: rete Enterprise e rete ISP.

Il protocollo ICMPv6:

- Neighbor & Router discovery
- Diagnostica e Address management
- address
  - Autoconfiguration
  - Modalità stateless
  - Modalità stateful (DHCPv6)
  - Stateless DHCPv6 (DHCPv6-lite)
- selezione del source e destination address negli host
- prefix delegation
- laboratorio:
  - Utilizzo, configurazione e verifica di PC windows per IPv6
  - verifica dei parametri di default configurati sul PC
  - configurazione del DNS
  - ping/trace ed accesso a servizi su server IPv6 only e dual stack
  - visualizzazione ed analisi di protocollo degli scambi di pacchetti con wireshark
  - alterazione delle policy table per modificare i percorsi di rete.

I principali protocolli di routing IGP in IPv6:

- RIPng
- EIGRPv6
- OSPFv3
- laboratorio:
  - configurazione di una rete Enterprise con eIGRP ed OSPFv3
  - configurazione di siti periferici con eIGRP
  - configurazione del backbone OSPFv3
  - configurazione della redistribuzione.

Meccanismi di transizione verso IPv6:

- Dual Stack
- tunnelling statico ed automatico
- Tunnel Broker
- Dual Stack-lite (DS-lite)
- meccanismi 6to4 e 6rd
- modello 6PE
- laboratorio:
  - configurazione di meccanismi di transizione
  - configurazione di tunnelling statico
  - utilizzo di tunnel broker e Tunnel Setup Protocol
  - configurazione di 6to4 e 6rd.

IPv6: istruzioni per l'uso

Il DNS per IPv6:

- differenze nel DNS ed IPv6 Resource Record
- AAAA glue e Recursive DNS Servers
- il problema del IPv6 brokenness ed il DNS whitelisting
- modalità di configurazione del DNS per gli host
- gestione delle viste: l'esempio Google
- esempio di configurazione di un Name Server: BIND 9.0.

Obiettivi

Al termine del corso i partecipanti:

- conosceranno nel dettaglio il funzionamento del protocollo IPv6
- saranno in grado di pianificare un piano di indirizzamento IPv6 sia in reti Enterprise che ISP
- sapranno ottimizzare il comportamento di IPv6 sugli host
- sapranno configurare il routing IPv6 su apparati Cisco.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente ISP.

Prerequisiti

Buona conoscenza dell'architettura di comunicazione TCP/IP e dei protocolli di routing IGP (RIP, eIGRP, OSPFv2). Per trarre il massimo beneficio dalle consistenti attività di laboratorio è utile possedere competenze di carattere pratico/operativo sulla configurazione di apparati Cisco.



IPv6 nelle reti ISP

Il corso descrive dettagliatamente le modalità di impiego di IPv6 in architetture ISP con backbone OSPFv3/IS-IS e BGP ed il meccanismo di transizione 6PE per l'integrazione di IPv6 con backbone ISP BGP/MPLS. Si descrive, inoltre, il modello 6VPE per la realizzazione di VPN IPv6 BGP/MPLS. Sono previste esercitazioni, sui temi trattati nella parte teorica, utilizzando un laboratorio costituito da router Cisco e Juniper, che emula l'architettura dei grandi backbone IP.
Rientra nei percorsi di certificazione Cisco CCIE Service Provider e Juniper JNCIE-SP.

Agenda (3 giorni)





Richiami su IPv6:

- indirizzamento, formato dell'intestazione e next-headers
- protocollo ICMPv6, Neighbor & Router discovery, diagnostica e Address Autoconfiguration
- DHCPv6 e DHCPv6-lite
- prefix delegation.

Aspetti di progetto delle reti ISP per IPv6:

- definizione di piani di numerazione IPv6
- scelta dell'architettura di routing: reti "IPv6-only" o riutilizzo dei backbone IPv4.

Routing IPv6 nelle reti ISP:

- OSPFv3: differenze con OSPFv2, funzionamento, configurazione
- IS-IS e le sue estensioni per IPv6
- BGP per IPv6.

Reti "IPv6-only": configurazione di una architettura di routing IPv6 nelle reti ISP.

Trasporto di pacchetti IPv6 su reti IP/MPLS:

- il modello 6PE
- trasporto di pacchetti iPv6 nelle VPN BGP/MPLS: il modello 6VPE
- implementazione in rete di 6PE e 6VPE.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- le architetture di routing utilizzate dagli ISP per il supporto di IPv6
- il ruolo e il funzionamento di OSPFv3, IS-IS e BGP nelle architetture di routing IPv6
- i modelli 6PE e 6VPE.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente ISP.

Prerequisiti

Conoscenza delle reti IP e esperienza di base di configurazione dei router Cisco per ciò che riguarda indirizzi IP e protocolli di routing.



Routing IPv6 nell'IOS XR Cisco

Il corso fornisce le competenze operative sulla configurazione base ed avanzata dei protocolli di routing IPv6 negli apparati Cisco *carrier-grade*, che utilizzano il sistema operativo IOS XR. Il corso focalizza l'attenzione sulle estensioni dei principali protocolli di routing utilizzati nelle reti dei Service Provider (OSPF, IS-IS, BGP). Saranno trattati i servizi di trasporto IPv6 nelle reti IPv4/MPLS.
È prevista una rilevante attività di laboratorio *hands on*, costituito da router Cisco basati su IOS XR e IOS.

Agenda (3 giorni)



Configurazioni base di IPv6 nell'IOS XR:

- indirizzi
- parametri del protocollo *Neighbor Discovery*
- alcuni comandi *Show* e *Debug*
- Access-list e Prefix-list IPv6.

Routing IPv6 nell'IOS XR:

- generalità
- Routing statico
- RIPng
- EIGRPv6
- estensioni IS-IS per IPv6
- BGP per IPv6.

OSPF versione 3 (OSPFv3):

- concetti generali
- confronto con OSPFv2
- Link State Advertisement (LSA)
- configurazione e *troubleshooting* nell'IOS XR.

Tunneling IPv6 in reti IPv4+MPLS:

- modello 6PE
- VPN IPv6 BGP/MPLS (6VPE)
- configurazione di 6PE e 6VPE nell'IOS XR.

Obiettivi

Al termine del corso i partecipanti saranno in grado di configurare in ambiente IOS XR, gli aspetti base ed avanzati dei principali protocolli di routing IPv6 utilizzati nelle reti dei Service Provider (OSPF, IS-IS, BGP) e i servizi di trasporto 6PE e 6VPE di IPv6 nelle reti IPv4/MPLS.

Destinatari

Tecnici e amministratori di rete responsabili dell'implementazione e gestione di reti Service Provider e Enterprise di medie/grandi dimensioni. Progettisti, system engineer, personale di supporto tecnico che hanno bisogno di conoscere le caratteristiche e la configurazione dei router Cisco con IOS-XR.

Prerequisiti

Per trarre pieno beneficio dal corso è richiesta una conoscenza generale delle reti IP: indirizzi IP, protocolli di routing fondamentali, e avere le conoscenze base sui temi trattati nel corso "IPv6: istruzioni per l'uso" (INP672).

IPv6 nel JUNOS Juniper

Il corso descrive l'implementazione IPv6 del JUNOS utilizzato nei router Juniper, con particolare riguardo ai protocolli di routing IGP ed EGP utilizzati per IPv6 e la loro configurazione. Sono previste esercitazioni di laboratorio sulla configurazione di router Juniper per realizzare diversi scenari di rete, sia 'IPv6 only' che di integrazione IPv6/IPv4.

Agenda (3 giorni)





Richiami su IPv6:

- indirizzamento, formato dell'intestazione e Next-headers
- protocollo ICMPv6, Neighbor & Router discovery, Diagnostica e Address Autoconfiguration.

Implementazione base nel JUNOS Juniper:

- configurazioni base
- parametri del protocollo Neighbor Discovery
- alcuni comandi Show e Traceoptions
- firewall Filter IPv6.

Routing IPv6 e implementazione JUNOS:

- RIPng
- Estensioni per IS-IS
- BGP per IPv6
- OSPFv3
- configurazione di RIPng, IS-IS, BGP e OSPFv3 nel JUNOS Juniper.

Trasporto di pacchetti IPv6 su reti IP/MPLS:

- il modello 6PE
- trasporto di pacchetti iPv6 nelle VPN BGP/MPLS: il modello 6VPE.
- configurazione di 6PE e 6VPE nel JUNOS Juniper.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- gli aspetti base dell'implementazione di IPv6 nel JUNOS
- la configurazione del routing IPv6 nel JUNOS
- l'implementazione JUNOS dei modelli 6PE e 6VPE.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente Juniper.

Prerequisiti

Conoscenza delle reti IP e esperienza di base di configurazione dei router Juniper per ciò che riguarda: indirizzi IP, protocolli di routing (OSPF, BGP), routing policy.



Evoluzione delle reti IP Broadband: fondamenti e linee guida

L'ecosistema delle telecomunicazioni ed il mondo Internet stanno rapidamente convergendo verso uno scenario ALL-IP, in cui servizi, applicazioni e contenuti saranno forniti esclusivamente su reti IP che sostituiranno completamente le attuali reti di TLC.
Il corso presenta l'evoluzione dell'architettura delle IP Broadband Network dei Telco, guidata dalla necessità:

- di competere con OTT/CP anche sui tradizionali business dei Telco (voce e messaggistica)
- di gestire i fortissimi incrementi di volumi, soprattutto legati a servizi video (streaming multicast e unicast) e alla diffusione dei servizi Cloud (per Business e Consumer)
- di fornire qualità per la terminazione del traffico IP adeguata al tipo di servizio e alle aspettative dei Clienti
- di migliorare le prestazioni (come ad esempio il throughput degli applicativi) rispetto alla terminazione 'best effort'
- di limitare l'incremento dei costi di rete e di abilitare ricavi incrementali sia da end user (servizi premium), sia da OTT/CP (servizi premium e revenue sharing) .

Per raggiungere questi risultati si deve modificare l'architettura delle reti IP che, per la maggior parte degli operatori di TLC:

- è di tipo centralizzato, sia per le funzionalità di IP Edge (come ad esempio Broadband Network Gateway e Broadband Remote Access Server), sia per i punti dai quali si inseriscono in rete i contenuti (content injection) dei servizi video e dei servizi Cloud
- utilizza IP/MPLS solo nel core della rete
- non consente di offrire qualità differenziata per la terminazione del traffico IP
- gestisce la qualità della terminazione IP solo con meccanismi basati su QoS e non utilizza piattaforme per migliorare la Quality of Experience (QoE).

L'approccio seguito da un numero crescente di Telco per realizzare le IP Broadband Networks per lo scenario ALL IP è basato su un'architettura distribuita e in particolare su

- realizzazione di una rete seamless IP/MPLS integrata (per fisso e mobile), che estende l'IP/MPLS dal core fino agli end user (seamless IP/MPLS), che consente la distribuzione dell'IP Edge e di Application Server
- distribuzione delle funzionalità di IP Edge, nei nodi di rete dove si effettua content injection (con piattaforme per migliorare la QoE, come ad esempio quelle di Content Delivery), sia per fornire la qualità differenziata richiesta dai servizi, sia per limitare l'incremento dei costi di rete
- inserimento di piattaforme per migliorare la QoE (Caching, TCP Optimization, Web Acceleration, CDN, ADN,…), che, oltre a ridurre il TCO di rete, consentono di offrire qualità differenziata, utilizzando il Policy Manager del traffico IP.

Agenda (3 giorni)

Evoluzione verso ALL IP: scenario di riferimento:

- competizione Telco-OTT (es. Web RTC, Skype, WhatsApp) e Telco-Telco
- cambiamenti nei modelli di business dei principali Player (Telco, OTT/CP, Carrier Internazionali) e nascita di nuovi Player (Content Delivery Provider)
- il "valore" della qualità per la terminazione IP (esempi: browsing, e-commerce, unicast video streaming, ricavi incrementali da UBB fisso e mobile, nuovi modelli di business)
- Quality of Service e Quality of Experience (Willingness to pay for QoE not for QoS)
- vantaggi dell'approccio basato su QoE rispetto all'approccio basato su QoS (miglioramento delle prestazioni e riduzione del TCO)
- nuovi modelli di business per i Telco. Monetizzazione degli accessi UBB e della terminazione del traffico generato da OTT/CP (da 'One Side Market' al 'Two Sides Market').

Piattaforme per migliorare la QoE:

- Bit rate e Application Throughput. Impatto della latenza sul Throughput e sulla QoE
- meccanismi per migliorare la QoE: caching, content and application delivery networks, protocol optimization, front end optimization
- CDN e Transparent Caching
- TCP Optimization
- Web Acceleration.

Evoluzione delle reti IP Broadband: fondamenti e linee guida

Architettura di riferimento nello scenario ALL IP per IP Broadband Networks:

- Seamless IP/MPLS su WDM
- integrazione dei livelli Trasporto e IP
- Network Functions Virtualization e Software Defined Networks
- distribuzione delle funzionalità di IP Edge
- inserimento in rete di piattaforme per QoE
- gestione del traffico IP basata sul Policy Control e sulle piattaforme per QoE
- come far evolvere la rete IP verso la ALL IP Broadband Network
- esempi di Network Cost Saving ottenuti con la distribuzione dell'IP Edge e con piattaforme di Content Delivery.

Case Studies:

- architettura 'as is' e 'to be' delle reti IP dei principali Telco (es. BT, Orange, DT, Verizon, AT&T)
- architettura delle reti degli OTT (es. Google, Amazon) e dei Content Delivery Provider (es. Akamai, L3).



Software Defined Networking (SDN), OpenFlow e Network Function Virtualization (NFV)

Le reti NGN, le nuove tecnologie di Software Defined Networking (SDN), OpenFlow e Network Function Virtualization (NFV) stanno alimentando un ampio dibattito tra gli esperti di networking.
Se l'intera industria IT si è mossa, negli ultimi dieci anni, verso soluzioni altamente automatizzate, mentre il mondo del networking è rimasto fermo al concetto di configurazione manuale dei singoli apparati. È così giunto il momento di ripensare al modello “manuale” e cambiare i processi operativi di deployment delle reti, riducendo la quantità di tempo spesa ad eseguire operazioni manuali ripetitive.
L’obiettivo di questo corso è dare alcune linee guida di alto livello. La presentazione si concentra sulle tecnologie di base SDN e NFV e il protocollo OpenFlow.

Agenda (2 giorni)





Software Defined Networking(SDN):

- motivazioni e principi fondamentali di SDN
- tecnologie abilitanti
- scenari di utilizzo
- dove, perché e come rendere una rete programmabile.

Introduzione a OpenFlow:

- piano di controllo e piano dati tradizionale
- Controller-based forwarding
- fondamenti del protocollo OpenFlow
- pro e contro di OpenFlow.

Scalabilità di OpenFlow:

- limitazioni hardware
- setup proattivo e reattivo delle tabelle di forwarding
- Hop-by-hop e path-based forwarding
- scalabilità del piano di controllo.

Casi reali di utilizzo di SDN.

Network Function Virtualization:

- la virtualizzazione delle funzioni di rete
- le iniziative di standardizzazione ed il ruolo dell’open source
- le tecnologie a supporto di NFV.

Sinergie SDN-NFV.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- l’evoluzione delle attuali reti IP verso reti programmabili
- i fondamenti del protocollo Openflow e i suoi aspetti di scalabilità
- gli aspetti principali della Network Function Virtualization e le sinergie SDN-NFV.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Buone conoscenze dell’architettura TCP/IP e dei principi del routing IP. Inoltre è richiesta una buona conoscenza delle architetture delle moderne reti IP.



Cloud Computing Networking

Negli anni più recenti, con l'introduzione delle nuove tecniche di virtualizzazione (di rete, degli *host*, dei *firewall*, ecc.), le tecnologie di *Data Center* hanno subito una rivoluzione tecnologica formidabile. Rivoluzione che sta generando nuove filosofie di rete (vedi il concetto di *Software-Defined Networking*, SDN) e nuovi protocolli (es. *OpenFlow*), destinati ad avere un impatto anche al di fuori del contesto dei *Data Center*.
L'argomento è tra i temi più attuali e questo corso risponde a domande di grande interesse, e mette in evidenza gli aspetti salienti e le criticità legati alla realizzazione di *Data Center* per i servizi di *Cloud Computing*.

Agenda (2 giorni)





Introduzione ai servizi Cloud:
- definizione di servizi Cloud
- IaaS, PaaS, SaaS …
- linee guida di progetto e implementazione.

Virtual networks:
- il perché delle virtual networks
- VLANs o overlay networks ?
- tecnologie per le Overlay Virtual Network.

Virtual appliances e firewalls:
- vantaggi delle virtual appliances
- Virtual firewall e router distribuiti.

Case study: VXLAN-based vCloud:
- principi e funzionamento delle VXLAN
- integrazione di VXLAN con virtual appliances
- Management e provisioning.

Data Center Transport Fabric:
- requisiti
- Trasporto Layer-2 o layer-3 ?
- architetture tipiche
- Leaf-and-spine (Clos) fabrics.

Case study: Programmable Flow:
- introduzione a SDN (Software-Defined Networking) e a OpenFlow
- componenti programmabili e principi di funzionamento
- Virtual tenant networks
- integrazione con i Cloud Provisioning Systems.

Architetture scalabili:
- Load Balancing locale e globale
- Disaster recovery and avoidance.

Obiettivi

Al termine del corso i partecipanti conosceranno:
- l'evoluzione delle attuali architetture dei Data Center verso il concetto di Overlay Virtual Networks
- le principali architetture di trasporto dei Data Center per i servizi cloud e le scelte sottostanti
- gli aspetti principali dell'evoluzione verso il controllo SDN.

Destinatari

Tecnici ed ingegneri di rete, (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'installazione e dell'amministrazione di reti di medie e grandi dimensioni.

Prerequisiti

Buone conoscenze dell'architettura TCP/IP e dei principi del routing IP. Inoltre è richiesta una buona conoscenza delle architetture delle moderne reti IP.

La Qualità del Servizio nelle reti IP

Il passaggio dalle tradizionali tecniche a commutazione di circuito, utilizzate quasi esclusivamente nel mondo telefonico, alle tecniche a commutazione di pacchetto, pone nuovi e complessi problemi di Qualità del Servizio, sia a livello di rete, che di sistemi.
Il corso presenta gli aspetti più importanti sulle problematiche di Qualità del Servizio nelle reti IP, le soluzioni tecnologiche proposte dagli Enti di standardizzazione, in particolare il modello Differentiated Services, e tutti i principali meccanismi utilizzati per differenziare il trattamento del traffico (classificazione e colorazione, controllo del traffico, gestione della banda e dei buffer, meccanismi di efficienza dei collegamenti). Una ampia e dettagliata sessione pratica illustra le modalità di configurazione della Qualità del Servizio in ambiente Cisco. Saranno infine presentati dei Case Studies di configurazioni su router in produzione.

Agenda (2 giorni)



Traffico e Qualità del Servizio nelle Reti IP:

- indici di Qualità del Servizio
- Delay budget
- modelli IETF di Qualità del Servizio (IntServ, DiffServ)
- interlavoro con la QoS a Livello 2
- il modello Differentiated Services
- meccanismi fondamentali
- per Hop Behaviour.

Meccanismi di Qualità del Servizio su reti IP:

- classificazione e colorazione del traffico
- gestione della banda (scheduling FIFO, WFQ, CBWFQ, LLQ, MDRR, ecc.)
- controllo del traffico (policing/shaping)
- gestione dei buffer (RED, WRED, ECN).

Aspetti di configurazione nei router Cisco:

- Modular QoS CLI (MQC)
- configurazione dei meccanismi di QoS nei router
- QoS negli Switch Layer 2.

Tecniche per migliorare l'efficienza dei collegamenti:

- compressione dell'intestazione
- frammentazione dei pacchetti.

Regole di Progettazione:

- Best Practice
- classificazione e Politiche di QdS
- Case Study finale.

Obiettivi

Illustrare le problematiche di Traffico e Qualità del Servizio nelle reti IP.
Illustrare i principali modelli architetturali, i meccanismi di Qualità del Servizio e fornire gli strumenti per valutarne l'applicabilità.
Applicare la teoria a problemi di dimensionamento e valutazione delle prestazioni.
Fornire gli elementi di base delle implementazioni dei meccanismi di QoS IP in ambiente Cisco.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP in ambiente enterprise e ISP.

Prerequisiti

Conoscenza generale delle reti IP e un minimo di esperienza di configurazione base dei router Cisco.



Cisco Voice over IP

Il corso fornisce le basi necessarie per svolgere attività operative su reti che utilizzano prodotti e soluzioni VoIP Cisco. Le tecnologie presentate sono quelle comunemente utilizzate sia in ambiente Enterprise che di Operatore pubblico di servizi IP Telephony (ITSP).
La descrizione teorica degli argomenti è completata da attività di laboratorio su apparati Cisco. In particolare sono utilizzati switch Catalyst e router Cisco per riprodurre situazioni analoghe a quelle realmente incontrate in reti VoIP di piccole e medie dimensioni.

Agenda (4 giorni)



Richiami su VoIP.

Architetture di rete VoIP.

Calcolo dei requisiti e allocazione di banda per una comunicazione VoIP.

Aspetti di sicurezza.

Aspetti di configurazione su apparati Cisco:

- Voice Ports
- Voice Interface Settings
- Dial Peers
- Voice Port Connections.

Segnalazione VoIP:

- H.323
- SIP
- MGCP
- MEGACO
- Confronto H.323-SIP
- Gatekepeer
- Architettura CUCM.

Installazione e configurazione dell'architettura H.323 su apparati Cisco.

Configurazione dell'architettura SIP su apparati Cisco.

Configurazione di MGCP su apparati Cisco.

Aspetti di Qualità della Voce (QOS).

La funzionalità di Call Admission Control (CAC).

Gatekepeer e gestione del dial-plane.

Architettura CUCM.

Obiettivi

Il corso fornisce le competenze che permettono ai partecipanti di:

- analizzare le caratteristiche di rete utili a fornire in modo integrato servizi voce e dati in ambienti differenti quali campus, enterprise e di operatori pubblici.
- effettuare le scelte corrette relativamente alla configurazione di apparati VoIP Cisco (tipo di interfaccia, tipo di codifica, tipo di segnalazione, ecc.).
- confrontare le principali tecnologie utilizzate nelle soluzioni VoIP.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP o di sistemi di fonia.

Prerequisiti

Protocolli di comunicazione e modello OSI, architetture di rete locale (LAN, bridging e switching) e di reti WAN, architettura TCP/IP, indirizzamento e subnetting, telefonia di base, segnalazione telefonica d'utente e di rete, concetti base su VoIP.

Voice over IP: architetture, protocolli e servizi

La migrazione del servizio di fonia dalle reti tradizionali, alle tecnologie VoIP, è ormai un processo inarrestabile. In molti paesi europei, ma soprattutto del sud est asiatico, una parte importante del traffico telefonico viaggia su reti IP. In generale con Voice over IP si intendono diverse modalità di trasferimento della voce su una rete IP, fra loro profondamente differenti, sia per l'utilizzo che per il grado di servizio. Si va dalle iniziali modalità PC-to-PC, fino a quelle più vicine alla telefonia tradizionale di tipo phone-to-phone, da una gestione della trasmissione di tipo best effort, all'utilizzo di protocolli specifici per l'instaurazione della sessione e la gestione della sicurezza e della qualità di servizio.

Agenda (4 giorni)

Scenari di mercato e tecnologici per il Voice over IP.

Codifica della voce.

Problematiche di trasporto della voce su reti IP.

Protocolli per il VoIP.

Il nuovo modello di centrale aperta.

MGCP e Megaco.

H.323.

SIP.

Il problema della QoS su reti IP:

- indici di valutazione delle prestazioni
- Delay Budget
- meccanismi di QoS.
- meccanismi di controllo di banda (CAC)

Gestione dei servizi VoIP nella rete di un operatore di TLC.

Backbone integrati multi servizio.

Scenari di Interlavoro tra rete telefonica/ISDN e rete IP.

Applicazioni VoIP per reti Corporate:

- IP Phone
- IP PBX.

Servizi avanzati su IP:

- Unified Messaging su IP
- Videoconferenza su IP.
- Presence and Unified Collaboration.

Aspetti di sicurezza:

- autenticazione
- cifratura del traffico
- cifratura della segnalazione.

Aspetti normativi.

Obiettivi

Il corso fornisce una visione ad ampio spettro delle alternative tecnologiche e architetturali dei servizi Voice over IP, con particolare enfasi agli aspetti applicativi, sia in ambito di reti corporate che nella rete di un operatore di TLC.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili della progettazione, dell'installazione, dell'amministrazione e del troubleshooting di reti IP o di sistemi di fonia.

Prerequisiti

Conoscenza delle reti telefoniche e dei protocolli TCP/IP.



IP-TV. La TV digitale sulle nuove reti dati

L'evoluzione delle reti di telecomunicazione a larga banda, sia in ambito locale che metropolitano, ha favorito lo sviluppo di servizi multimediali e la convergenza con i servizi tradizionali. Originariamente sviluppate per la trasmissione dati e i servizi internet, le reti Ethernet e IP oggi sono sempre più utilizzate per la integrazione di servizi quali la fonia e la televisione, che ne sfruttano le potenzialità e la flessibilità.
Nel corso si illustra l'implementazione di servizi di televisione digitale su reti per dati, sia da parte di operatori di TLC, nell'ottica di realizzare il cosiddetto modello Triple Play, sia da parte di aziende che vogliono sfruttare la propria rete dati per veicolare servizi di Business Television (BTV).

Agenda (2 giorni)

La TV digitale:

- il segnale televisivo analogico e digitale
- codifiche video: MPEG
- modalità di trasmissione del segnale video
- DVB e VoD
- alternative tecnologiche per la TV digitale
- Web TV e IP-TV
- servizi multimediali interattivi.

Tecnologie di rete per l'implementazione del servizio IP-TV.

Protocolli per l'IP-TV:

- richiami alle tecnologie Ethernet e Gigabit Ethernet
- richiami al protocollo IP e alla trasmissione multicast su IP
- il problema della QoS.

Soluzioni architetturali per l'IP-TV:

- canali Live
- video on demand
- set-Top-Box: architettura HW e SW
- Centro Servizi Video
- configurazioni di rete.

Le strategie degli operatori sui servizi IP-TV ed esempi di offerte commerciali.

Obiettivi

Al termine del corso i partecipanti conosceranno:

- le funzionalità della TV digitale
- le modalità di realizzazione di servizi televisivi digitali su una infrastruttura dati basata sul protocollo IP, sia essa di un operatore di TLC che di una singola azienda.

Destinatari

Responsabili e tecnici di rete, progettisti e consulenti di progetti ICT.

Prerequisiti

Conoscenze di base sui protocolli per la trasmissione dati.

Segnalazione su IP: SIP e DIAMETER

La forte tendenza in atto verso la migrazione dei servizi voce, tradizionali e avanzati e l'implementazione di applicazioni multimediali su reti IP, unitamente all'affermarsi del modello NGN (Next Generation Network), hanno reso necessario definire dei protocolli di segnalazione specifici per il corretto funzionamento di tali servizi mediante il paradigma previsto dall'IP.
Il corso illustra le procedure (ad es. attivazione di una sessione, gestione della QoS, profilazione dell'utente e tariffazione) previste per i vari SoIP (Service over IP) e i protocolli utilizzati dalle attuali piattaforme di rete con particolare riferimento a SIP e Diameter. Grande spazio è dato alle esercitazioni pratiche, con numerosi esempi ed analisi di tracciati reali.

Agenda (3 giorni)



Richiami sulla segnalazione CCS7.

Richiami sul protocollo IP.

Segnalazione SIP:

- concetto di sessione e di connessione
- User Agent Client e User Agent Server
- architettura funzionale del sistema SIP: terminali, proxy server, B2BUA, registrar, location service
- modello base di una chiamata SIP
- SIP URI e Enum
- confronto tra una connessione fonica ed una sessione SIP
- transazione e dialogo di segnalazione
- struttura dei messaggi SIP: messaggi di richiesta, messaggi di risposta
- esempio di un messaggio INVITE
- analisi di un tracciamento di un Session Set up SIP.

Procedure del protocollo SIP:

- esempi:
- registrazione
- session setup tra terminali in una rete LAN collegati direttamente
- session setup tra terminali collegati attraverso dei proxy server.

Analisi di casi particolari in cui si verificano anomalie.

Segnalazione SIP nelle reti radiomobili:

- accesso ai proxy server mediante la rete UMTS Packet Switching
- integrazione tra la segnalazione SIP e ISUP
- analisi di protocollo di una chiamata voce tra terminale mobile e PC.

Il protocollo DIAMETER:

- protocollo Base Diameter
- confronto tra Diameter e Radius
- struttura dei messaggi
- comandi
- elenco degli Attributi (AVP) di base e sviluppati per IMS
- il ruolo di Diameter nelle reti IP.

Obiettivi

Presentare le caratteristiche principali dei protocolli più utilizzati nelle reti IP multimediali.
Analizzare il funzionamento dei protocolli illustrati nelle principali procedure per l'attivazione e la gestione di un servizio.

Destinatari

Responsabili e tecnici di Planning e Operation, responsabili e tecnici ISP, fornitori di apparati e sistemi, Personale tecnico coinvolto nelle forniture di servizi avanzati.

Prerequisiti

Conoscenza delle reti telefoniche, delle reti per dati e delle caratteristiche principali del protocollo IP.



SIP: architetture, protocollo e servizi

Il protocollo SIP (Session Initiation Protocol) si è affermato come il paradigma di riferimento per la segnalazione nella implementazione di servizi voce e multimediali su reti IP, soprattutto da quando è stato adottato come protocollo di comunicazione fra le varie entità delle piattaforme di controllo (quali IMS in primis e TISPAN) delle reti NGN (Next Generation Networks).
Il corso descrive le principali caratteristiche di SIP, le tipiche architetture di rete e d'utente per la realizzazione e fornitura di servizi avanzati di comunicazione. Vengono poi presentati e discussi vari esempi di uso di SIP (e dei linguaggi basati su XML) per realizzare servizi e funzionalità di IP Telephony.

Agenda (3 giorni)

Richiami sulle reti, sulle architetture e sui servizi VoIP.

Introduzione al protocollo e alla terminologia SIP.

Indirizzamento SIP (Formalismo delle SIP URI, Enum).

Il modello protocollare Client-Server di SIP.

Richieste e Risposte del protocollo SIP "di base" (RFC 3261).

SDP (Session Description Protocol).

Protocolli per i "media" abilitati da SIP / SDP (RTP, MSRP, ecc.).

Il concetto di "dialogo SIP e quello di "sessione".

Registrazione e "Nomadismo" in reti SIP. Protocolli per il trasporto di SIP "over IP ".

Principali tipi di "ruoli" (blocchi funzionali) SIP:

- User Agent (UA) e Registrar
- Proxy Stateless, Proxy Transaction Stateful, Proxy Call Stateful, Proxy Service Stateful
- Forking Proxy
- AS (Application Server), B2BUA
- Gateway(s).

Transazioni. Forking.

Approfondimenti sui meccanismi di "Routing" di livello SIP:

- utilità dei DNS (Domain Name Server) in una rete SIP; possibili alternative.

Rassegna dei principali "Header" usati per il routing di SIP e per realizzare servizi.

Esempi di interlavoro tra reti SIP, SS7 ed H323.

SIP ed XML, SIP ed http.

Scripting Languages basati su XML (Javascripts, CPL, ecc.,).

Aspetti di sicurezza in SIP, cenni alle tecniche crittografiche.

Aspetti di Reliability e "QoS" in reti SIP.

Estensioni del protocollo SIP di fonte IETF o 3GPP.

Esempi di possibili modi per realizzare con SIP alcuni servizi supplementari.

Cenni all'implementazione e all'uso di SIP nelle reti attuali (Reti di operatori fissi e mobili, Reti "Corporate").

Cenni alla architettura "IMS", un'architettura del 3GPP basata su SIP.

Obiettivi

Approfondire le caratteristiche del protocollo SIP e il suo ruolo nella implementazione di servizi multimediali su reti IP.

Destinatari

Responsabili e tecnici di Planning e Operation, responsabili e tecnici ISP, fornitori di apparati e sistemi, personale tecnico coinvolto nelle forniture di servizi avanzati, manager di rete.

Prerequisiti

Conoscenza delle reti telefoniche, delle reti per dati e del protocollo IP.



IMS: architettura e applicazioni in ottica NGN

L'IMS (IP Multimedia SubSytem) è la proposta del 3GPP (Third Generation Partnership Project) di una piattaforma di controllo per la realizzazione di servizi multimediali avanzati attraverso una rete IP, con accesso fisso, mobile o nomadico, ma soprattutto convergente, in ossequio al modello di rete NGN (Next Generation Networks). Si usa dire che IMS è "access agnostic" ad indicare la sostanziale indipendenza del controllo dei servizi dalla piattaforma trasmissiva. Il corso è incentrato sul modello delle reti NGN di separazione del controllo dei servizi, dal trasporto delle informazioni e sul ruolo fondamentale di IMS in questa architettura. Sono descritti i blocchi funzionali dello standard, la loro interazione e la implementazione fisica negli apparati di rete. Particolare enfasi è data alle modalità di implementazione dei servizi multimediali attraverso IMS e agli aspetti di interlavoro fra reti di operatori differenti.

Agenda (3 giorni)

Richiami alle tecnologie per telefonia e dati.

Evoluzione delle reti core fisse e mobili: verso l'IMS.

Architettura "core" IMS: blocchi funzionali (CSCF, HSS, BGCF, MRFC/P, AS...).

Interfacce fra i blocchi funzionali IMS.

IPv4 e IPv6 in IMS. Richiami al protocollo SIP.

Funzionalità SIP dei principali blocchi funzionali di IMS. Estensioni di SIP di base per IMS.

Potenzialità e prestazioni dei layer IMS di controllo e servizio, in reti NGN.

Interlavoro di IMS con reti tradizionali TDM (fisse e mobili), e con reti IMS di altri Carrier interconnessi "over IP".

Aspetti di accounting, billing e sicurezza.

Nomadismo dell'utente IMS:

- evoluzione rispetto alle modalità tradizionali SIP
- identità multiple, terminali multipli.

Servizi (o "enablers").

Principali funzionalità di "estensione" specificate dal 3GPP per gli operatori TLC tradizionali:

- sicurezza, compressione della segnalazione, accounting inter IMS-carriers, gestione della QoS.

Interlavoro tra reti IMS e reti a puro standard SIP.

Il ruolo di IMS nell'evoluzione delle reti intelligenti tradizionali.

XML in IMS per forme di comunicazione avanzata:

- servizi di "presence"
- customer creation environment
- buddy lists, transazioni
- collaborative browsing.

Soluzioni complementari od alternative ad IMS:

- piattaforme di comunicazione web-oriented
- IMS e l'approccio Peer to Peer.

Apertura di IMS a terze parti: limiti dell'approccio IMS " verso l'alto".

Obiettivi

Presentare la filosofia delle reti NGN e il ruolo svolto dall'IMS nella separazione funzionale tra le applicazioni e la rete. I partecipanti avranno un quadro esaustivo delle possibili funzionalità dell'IMS per la implementazione dei servizi multimediali.

Destinatari

Responsabili e tecnici di rete, fornitori di apparati e sistemi, personale tecnico coinvolto nelle forniture di servizi avanzati.

Prerequisiti

Conoscenza delle reti telefoniche, delle reti per dati e delle principali caratteristiche del protocollo IP.



Avaya Aura Communication Manager: Design, Configurazione e Troubleshooting

Avaya Aura Communication Manager consente di organizzare e instradare le trasmissioni di fonia, dati, immagini e video. È collegabile a reti telefoniche private e pubbliche, reti locali Ethernet e a Internet.
Communication Manager si prefigge di soddisfare le esigenze delle aziende offrendo comunicazioni vocali integrate con applicazioni a valore aggiunto. È un'applicazione di telefonia aperta, scalabile, altamente affidabile e sicura. Fornisce le funzionalità per gli utenti e per la gestione del sistema, l'instradamento intelligente delle chiamate, l'integrazione e l'ampliamento con altre applicazioni e la connessione in rete per le comunicazioni aziendali.

Agenda (3 giorni)

Avaya Aura Overview.

Avaya Server.

Avaya Gateway.

Avaya Aura Common Server.

Avaya Aura CM Templates.

Duplication Survivability and Reliability.

Overview of telephones.

Avaya Site Administration (ASA).

Basic command structure.

Dial Plan.

Feature Access Code.

Digital and analog telephones.

IP telephones.

Class Of Service.

Class Of Restriction.

Calling Permission.

Bridged Call Appearance

Automatic Alternate Routing (AAR).

Automatic Route Selection (ARS).

Trunk Type.

ISDN PRI.

Backup.

Real Time Monitoring.

Reports.

Obiettivi

Overview dei prodotti Avaya Aura e formazione tecnica di base su architettura Avaya Aura Communication Manager.

Destinatari

Responsabili e tecnici di rete, fornitori di apparati e sistemi, System Integrator, tecnici installatori.

Prerequisiti

Conoscenza della telefonia analogica o IP, TCP/IP.



Asterix

Il corso è pensato per sviluppare una conoscenza teorica e soprattutto pratica di progettazione, installazione e configurazione di un centralino basato su tecnologia Asterisk. Sono presentate e approfondite le tecnologie ed il software necessario a sviluppare un sistema PBX basato su Asterisk operante sotto GNU/Linux. Gli argomenti chiave, descritti di seguito, includono le basi necessarie ad affrontare le tecnologie specifiche, gli strumenti per le personalizzazioni e le configurazioni avanzate per la sua messa in opera in realtà aziendali.

Agenda (4 giorni)





Cenni sui Sistemi Operativi GNU/Linux.

Cos'è Asterisk.

Protocolli voip e Terminal Equipment.

Preparare all'Installazione di Asterisk. Installare e configurare Asterisk.

Creare un DIAL PLAN.

Call Monitoring.

Asterisk "Preconfezionato": le alternative.

Manutenzione e Sicurezza.

Esercitazione pratiche per Small Office e Home Office.

Gestione avanzata del DIAL PLAN: Extention, Action, Macro, dial pattern.

Gestione delle priorità, convenzioni e caratteri speciali.

Funzioni avanzate (parcheggio delle chiamate, conferenza, find-me e follow-me, musica d'attesa).

Gestione scripting complessi direttamente da DIAL PLAN.

Costruzione ed implementazione IVR (Interactive Voice Response).

Monitoraggio e registrazione delle chiamate.

Approfondimenti dei protocolli voip e cenni di Networking.

Relazionare più centralini Asterisk.

Connessione ad un VOIP provider.

Code di chiamata e ACD (Automatic Call Distribution).

Interazione di Asterisk con un database. Gestione avanzata del Call Detail Record.

Connessione al centralino via Bluetooth.

Sistemi ad alta affidabilità (clustering e load balancing) e virtualizzazione.

Interfacciamento verso centrali telefoniche (PABX).

Obiettivi

Al termine del corso i partecipanti avranno sviluppato le competenze necessarie a realizzare PBX voip basati su Asterisk. Saranno capaci di personalizzare l'installazione di Asterisk sulle necessità aziendali e sapranno gestire la manutenzione ordinaria e straordinaria di un centralino basato su Asterisk.

Destinatari

Amministratori di rete o sistemisti di centralini aziendali su Asterisk
Tecnici ed installatori di centralini e PBX Asterisk
System Integrators di centralini aziendali Asterisk

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base:

- principi di base di networking
- stack di protocolli TCP/IP
- principi di voip

CCNA Voice

Il corso CCNA Voice certifica le capacità necessarie per gestire l'architettura, i componenti, le funzionalità degli apparati che costituiscono gli elementi fondamentali di Cisco Unified Communications Architecture: la soluzione offerta da Cisco Systems che permette la convergenza video e voce in unica, robusta e flessibile soluzione destinata all'implementazione da parte di grandi e medie aziende. Verranno esaminati le caratteristiche dei principali apparati: Cisco Unified Communication Manager (CUCM), Cisco Unified Communication Manager Express, Cisco Unity Connection, Cisco Unified Presence e come interagiscono i vari applicativi a supporto.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 640-461 ICOMM v8.0.

Agenda (5 giorni)





Descrivere le caratteristiche della soluzione di Cisco Unified Communications:

- descrivere le componenti e le funzioni delle soluzioni Cisco Unified Communications
- descrivere il call signalling e il media flows
- descrivere le implicazioni di quality di una rete VoIP.

Provision end users e devices:

- descrivere le opzioni per la creazione degli utenti per le soluzioni Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- creare e modificare gli user accounts per il Cisco Unified Communications Manager
- creare e modificare gli user accounts per il Cisco Unified Communications Manager Express usando la GUI
- creare e modificare gli endpoints per il Cisco Unified Communications Manager
- creare e modificare gli endpoints per il Cisco Unified Communications Manager Express usando la GUI
- descrivere le funzioni di calling privileges e come impattano le features di sistema
- creare e modificare i directory numbers
- abilitare le user features e I relativi calling privileges per extension mobility, call coverage, intercom, native presence, e unified mobility remote destination configuration
- abilitare gli end users per il Cisco Unified Presence
- verificare user features.

Configurare voice messaging e presence:

- descrivere user creation options per il voice messaging
- creare e modificare user accounts per il Cisco Unity Connection
- descrivere le soluzioni di Cisco Unified Presence
- configurare il Cisco Unified Presence.

Monitorare il sistema Cisco Unified Communications:

- generare i reports CDR and CMR
- generare capacity reports
- generare usage reports
- generare RTMT reports per monitorare le attività del sistema
- monitorare l'uso della voicemail
- rimuovere unassigned directory numbers
- perform manual system backup.

Fornire il supporto end user:

- verificare la connettività PSTN
- troubleshooting endpoint
- identificare voicemail issues e risolvere issues degli user mailboxes
- descrivere le cause e I sintomi di call quality issues
- reset single devices
- descrivere come usare le phone applications.

CCNA Voice

Laboratorio:

- attivazione dei servizi di base sul CallManager
- registrazione terminali sul CallManager, classi di servizio e dial-plane
- attivazione dei servizi di base sul CallManager Express
- registrazione terminali e servizi sul CallManager Express
- attivazione Cisco Unity Connection: sincronizzazione con il CallManager e voice mail utenti
- strumenti di monitoraggio.

Obiettivi

Fornire le competenze necessarie per amministrare una rete telefonica basata su protocollo IP. Preparare i partecipanti a diventare delle figure professionali in grado di avere i requisiti necessari per comprendere e trattare tecnologie di telecomunicazione VoIP in generale e in particolare sulle soluzioni di Unified Messaging e di Unified Presence.

Destinatari

Tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Conoscenza generica del mondo LANs, WANs, e IP switching/ routing.

Voice Communications and QoS in ambiente Cisco

Il corso fornisce le nozioni pratiche e teoriche per implementare e operare su gateways, gatekeepers, Cisco Unified Border Element, Cisco Unified Communications Manager Express e per configurare meccanismi di QoS in un'infrastruttura voce Cisco.
È parte del percorso formativo per conseguire la certificazione CCNP Voice e fornisce la preparazione necessaria per sostenere l'esame di certificazione "Implementing Cisco Unified Communications Voice over IP and QoS" (Esame Cisco 642-437 CVOICE v8.0).

Agenda (5 giorni)





Componenti principali di una rete VoIP e protocolli utilizzati.

Requisiti fondamentali per le comunicazioni VoIP e tipi di codec.

La configurazione dei gateway per le chiamate VoIP e PSTN.

Esercitazione a gruppi su laboratorio remoto: configurazione di dial peer e voice port.

Alcuni dettagli sui protocolli di segnalazione utilizzati nei voice gateway:H.323, SIP, MGCP.

Comandi di configurazione dei Gateway VoIP per l'utilizzo dei protocolli di segnalazione.

Esercitazione a gruppi su laboratorio remoto: configurazione di Gateway VoIP.

Definizione da un Dial Plan.

Descrizione di ciascuna componente di un Dial Plan.

Funzioni di un Gatekeeper H.323.

Ruolo dei Gatekeeper per la risoluzione di Dial Plan e per il Call Admission Control (CAC).

Esercitazione a gruppi su laboratorio remoto: implementazione di un Dial Plan su Gateway VoIP e configurazione di un Gatekeeper per CAC.

Implementazioni di gateway Cisco Unified Border Element (CUBE) per l'interconnessione con un Internet Telephony Service Provider.

Esercitazione a gruppi su laboratorio remoto: implementazione di gateway CUBE.

Simulazione di un esame CVOICE.

Obiettivi

Il corso fornisce le competenze per:

- comprendere il funzionamento di un voice gateway con tutte le sue caratteristiche e features associate
- interpretare le caratteristiche e gli elementi di un VoIP call legs
- implementare un dial-plan
- comprendere il funzionamento di un Gatekeepers e un Cisco Unified Border Elements
- comprendere il funzionamento della QoS, soprattutto in ambiente Cisco e sapere implementare i meccanismi principali per la corretta riuscita del setup-voce.

Destinatari

Il corso è rivolto a tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Confidenza con i concetti base e i termini legati al mondo del networking e dell' IP e nello specifico conoscenza generica del mondo LANs, WANs, e IP switching/ routing.

Cisco Unified Communications Manager: Base

Il corso è focalizzato sulla soluzione Cisco Unified Communication Manager e prepara all'implementazione di questa soluzione in un ambiente con singolo sito. Fornisce le nozioni teorico pratiche per eseguire una corretta progettazione da un dial-plan fino all'interfacciamento con gateway di diversi protocolli quali il Media Gateway Control Protocol (MGCP) e H.323.
È parte del percorso formativo per conseguire la certificazione CCNP Voice e fornisce la preparazione necessaria per sostenere l'esame di certificazione "Implementing Cisco Unified Communications Manager, Part 1" (Esame Cisco 642-447 CIPT1 v8.0).

Agenda (5 giorni)





Introduzione a Cisco Unified Communications Manager (CUCM):
- architettura
- installazione, aggiornamenti e aspetti di fault-tolerance
- requisiti per l'utilizzo di DHCP, TFTP, DNS e NTP.

Esercitazione a gruppi su laboratorio remoto.

Amministrazione del CUCM per chiamate Single-Site On-Net:
- configurazione di utenti, gruppi di utenti, supporto di Cisco SCCP e telefoni SIP, integrazione con LDAP
- sicurezza dei telefoni IP
- configurazione di switch per il supporto di telefoni IP
- utilizzo del Bulk Administration Tool (BAT) per la gestione di utenti e telefoni e descrizione delle funzioni del Tool for Auto-Registered Phones Support (TAPS).

Esercitazione a gruppi su laboratorio remoto.

Amministrazione del CUCM per chiamate Single-Site Off-Net:
- implementazione di un Gateway MGCP
- configurazione di route patterns, route filters, route list e route group
- strumenti per la prevenzione delle frodi
- implementazione di privilegi e copertura delle chiamate.

Esercitazione a gruppi su laboratorio remoto.

Implementazione di Media Resources, Features e Applicazioni:
- descrizione di Media resources
- risorse HW e SW per l'audioconferenza
- configurazione di MoH, MRG e MRGL
- interazione con sistemi di voice-mail.

Esercitazione a gruppi su laboratorio remoto.

Sintesi degli argomenti trattati e sessione di domande.

Obiettivi

Il corso fornisce le competenze per:
- saper progettare e implementare una soluzione completa con il Cisco Unified Communications Manager, facendo tuning di tutte le opzioni configurabili per ottimizzare l'architettura stessa e sfruttare le applicazioni ad esso associate
- costruire un dial-plan intelligente
- implementare un Cisco Unified Communications Manager media resources.

Destinatari

Il corso è rivolto a tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Confidenza con i concetti base e i termini legati al mondo del networking e dell' IP e nello specifico conoscenza generica del mondo LANs, WANs, e IP switching/ routing.

Cisco Unified Communications Manager: Avanzato

Il corso prepara alla progettazione e implementazione della soluzione Cisco Unified Communications in un ambiente composto da più siti. Esso copre concetti di call routing globalizzato come il Cisco Service Advertisement Framework (SAF), il Call Control Discovery (CCD), il tail-end hop-off (TEHO), il Cisco Unified Survivable Remote Site Telephony (SRST) e concetti di mobilità e di emergenza in caso di caduta di connessioni WAN.
È parte del percorso formativo per conseguire la certificazione CCNP Voice e fornisce la preparazione necessaria per sostenere l'esame di certificazione "Implementing Cisco Unified Communications Manager, Part 2" (Esame Cisco 642-457 CIPT2 v8.0).

Agenda (5 giorni)





Implementazione di scenari IP Telephony Multisite:
- problemi e soluzioni
- implementazione di connessioni multisite
- implementazione di un piano di numerazione per connessioni multisite.

Esercitazione a gruppi su laboratorio remoto.

Implementazione di scenari IP Telephony con Call Processing centralizzato:
- opzioni di fault-tolerance
- implementazione di SRST (Cisco Survivable Remote Site Telephony)e MGCP fallback
- implementazione di CUCM Express in modalità SRST.

Esercitazione a gruppi su laboratorio remoto.

Implementazione della Bandwidth Management e del Call Admission Control.

Esercitazione a gruppi su laboratorio remoto.

Implementazione di features e applicazioni in scenari IP Telephony Multisite.

Configurazione della mobilità (device, extension, unified mobility).

Esercitazione a gruppi su laboratorio remoto.

Aspetti di sicurezza in IP Telephony:
- descrizione tipi di attacco a una rete VoIP e contromisure
- aspetti di cifratura e PKI
- funzionalità native di sicurezza nei CUCM e CUCM PKI
- implementazione della sicurezza nei CUCM.

Esercitazione a gruppi su laboratorio remoto.

Sintesi degli argomenti trattati e sessione di domande.

Obiettivi

Il corso fornisce le competenze per:
- implementare un call routing globalizzato e meccanismi di SAF, TEHO, CCD
- implementare meccanismi di sopravvivenza di un sito quali il CAC, AAR, SIP precondition
- ottimizzare la banda WAN con meccanismi di filtri e features varie
- implementare la mobilità degli utenti come Extension Mobility e il Device Mobility.

Destinatari

Il corso è rivolto a tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Confidenza con i concetti base e i termini legati al mondo del networking e dell' IP e nello specifico conoscenza generica del mondo LANs, WANs, e IP switching/ routing.



Troubleshooting Unified Communications in ambiente Cisco

Il corso è parte del percorso formativo per conseguire la certificazione CCNP Voice (CCNP Voice) e fornisce la preparazione necessaria per sostenere l'esame di certificazione "Troubleshooting Cisco Unified Communications" (Esame Cisco 642-427 TVOICE v8.0).

Agenda (5 giorni)





Metodologie per il Troubleshooting:

- descrizione dei possibili passi da utilizzare per identificare problemi di funzionamento
- strumenti per identificare e isolare i problemi di funzionamento
- correlazione di eventi (utilizzo di trace, log, strumenti di monitoraggio).

Esercitazione a gruppi su laboratorio remoto.

Troubleshooting di CUCM:

- troubleshooting dei meccanismi di fault-tolerance
- troubleshooting dei meccanismi di sicurezza
- troubleshooting di Database e LDAP replication
- troubleshooting di problemi di registrazione (Gateway e Gatekeepers).

Esercitazione a gruppi su laboratorio remoto.

Troubleshooting di call setup:

- troubleshooting di PSTN call setup
- troubleshooting di intersite e intrasite call setup.

Esercitazione a gruppi su laboratorio remoto.

Troubleshooting di qualità della voce e del video:

- problemi di eco
- problemi di caduta delle conversazioni
- problemi di qualità dell'audio
- troubleshooting di problemi di qualità del Cisco Unified Video Advantage.

Esercitazione a gruppi su laboratorio remoto.

Troubleshooting di problemi di integrazione delle applicazioni e media resources:

- problemi di integrazione con voice-mail
- problemi di Computer Telephony Integration (CTI)
- problemi di media resources (MoH, transcoders, conference bridges, ecc.).

Esercitazione a gruppi su laboratorio remoto.

Sintesi degli argomenti trattati e sessione di domande.

Obiettivi

Il corso fornisce le competenze per:

- analizzare le caratteristiche dei servizi voce includendo importanti features come Call Control Discovery, SIP Precondition, Extension Mobility Cross Cluster, problemi con il dial plan o il call routing
- individuare e saper correggere problemi che possono insorgere in fase di registrazione degli end-points, dei gateway e in generale problemi generici con il call setup di una chiamata
- saper correlare traces, logs, debugs e output di vari monitoring tools.

Destinatari

Il corso è rivolto a tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Protocolli di segnalazione e nozioni generali sulla piattaforma Cisco Unified Communications v8.0.

Cisco Unified Communications Applications

Il corso illustra come integrare Cisco Unified Presence, Cisco Unity Express, and Cisco Unity Connection. Descrive gli scenari evolutivi della messaggistica vocale, le caratteristiche di Cisco Unified Presence e gli aspetti di troubleshooting, le modalità di integrazione di Cisco Unified Presence e Cisco Unified Personal Communicator con Cisco Unified Communications Manager.
È parte del percorso formativo per conseguire la certificazione CCNP Voice e fornisce la preparazione necessaria per sostenere l'esame di certificazione "Integrating Cisco Unified Communications Applications v8.0", (Esame Cisco 642-467 CAPPS v8.0).

Agenda (5 giorni)





Introduction to Voice Mail.

Cisco Unity Connection in a Cisco Unified Communications Manager Environment.

Cisco Unity Express Implementation in Cisco Unified Communications Manager Express Environment.

Voice Profile for Internet Mail Implementation.

Cisco Unified Presence Implementation.

Esercitazione a gruppi su laboratorio remoto.

Sintesi degli argomenti trattati e sessione di domande.

Obiettivi

Fornire la preparazione necessaria per sostenere l'esame di certificazione "Integrating Cisco Unified Communications Applications v8.0" (Esame Cisco 642-467 CAPPS v8.0).

Destinatari

Il corso è rivolto a tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti integrate voce-dati.

Prerequisiti

Protocolli di segnalazione e nozioni generali sulla piattaforma Cisco Unified Communications v8.0.



ITIL® v3: Overview per Manager

Il framework ITIL® (*Information Technology Infrastructure Library*) è un insieme di linee guida e best practice per la gestione di servizi IT di qualità e fornisce indicazioni sui processi e sui mezzi necessari a supportarli.
La sua implementazione porta all'azienda numerosi e reali vantaggi, come la riduzione dei costi nell'erogazione dei servizi, il miglioramento della qualità e la soddisfazione dei bisogni correnti e futuri del business e dei clienti.

Agenda (1 giorno)

Introduzione a ITSM (IT Service Management).

Introduzione a ITIL® (IT Infrastructure Library).

Il nuovo concetto di ITIL® Service Management Lifecycle.

I capisaldi del paradigma ITIL® v 3.

Service Strategy.

Service Design.

SLA Service Level Agreement.

Definizione dei servizi.

Security e service continuity.

Service Transition:

- change management
- gestione della configurazione
- rilascio e implementazione.

Service Operation:

- gestione degli eventi
- soddisfazione dei requisiti.

Continual Service Improvement.

Il rapporto di ITIL con altri framework e standard:

- COBIT, ISO/IEC 20000, ISO/IEC 15504
- Risk Management
- Project Management (PMBOK e PRINCE2)
- CMMI
- Six Sigma.

Adattamento di ITIL alla realtà aziendale.

Obiettivi

Acquisire una buona conoscenza delle best practices ITIL e comprendere i vantaggi con l'introduzione di ITIL nei processi aziendali.

Destinatari

Direttori e Responsabili ITC, Responsabili di progetti e di servizi IT, Responsabili Qualità e Organizzazione.

Prerequisiti

Nessuno.



ITIL® v3 Foundation

Il framework ITIL® (*Information Technology Infrastructure Library*) è un insieme di linee guida e best practice per la gestione di servizi IT di qualità e fornisce indicazioni sui processi e sui mezzi necessari a supportarli. Con il rilascio della versione 3.0 il "core" di ITIL si costituisce di cinque pubblicazioni che specificano le caratteristiche dei processi di base per un'implementazione dei servizi di gestione dell'IT solida e ad alto livello.
Gli obiettivi che si pone ITIL v.3.0 Foundation sono:

- allineare i servizi IT con i bisogni correnti e futuri del business e dei clienti
- migliorare la qualità dei servizi IT erogati
- ridurre i costi fissi di erogazione dei servizi.

Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione e si conclude con l'esame "ITIL v3 Foundation". Il superamento dell'esame fornisce 2 crediti nel percorso di certificazione "ITIL v3 Expert".

Agenda (3 giorni)





Introduzione: lo schema di certificazione ITIL v3.- ITIL 2011

Definizione dei concetti di base: le fasi del ciclo di vita.

Service Strategy:

- gestione e implementazione della strategia IT
- gestione della domanda.

Service Design:

- gestione del Service Level Agreement (SLA)
- definizione del catalogo dei servizi
- sicurezza delle informazioni e continuità del servizio.

Service Transition:

- change management
- gestione della configurazione
- rilascio e implementazione.

Service Operation:

- gestione degli eventi
- gestione degli incidenti
- change management
- soddisfazione dei requisiti.

Continual Service Improvement.

Ruoli e responsabilità.

Preparazione all'esame e simulazione esame.

Esame di certificazione.

Obiettivi

Acquisire una buona conoscenza delle best practices ITIL ed una preparazione per il conseguimento della certificazione "ITIL v3 Foundation".

Destinatari

Responsabili dei servizi IT, IT Manager, Network Manager, IT Specialist, Responsabili di Progetto e Responsabili Qualità.

Prerequisiti

Nessuno.



ITIL® V3 Intermediate

In questa scheda sono descritti i corsi che consentono di realizzare il processo di certificazione ITIL® di livello intermediate, il percorso è articolato in più moduli, ognuno con un diverso focus e ognuno corrispondente a una diversa certificazione.
La scelta del numero e del tipo di certificazioni sarà fatta da ciascuno in base ai propri interessi e alle proprie motivazioni. Ogni esame consente di conseguire una parte dei 22 crediti richiesti per poter affrontare la certificazione "ITIL v3 Expert".
È possibile scegliere tra due percorsi.
Service Lifecycle con i seguenti moduli formativi e relative certificazioni:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement.

Ognuno di questi moduli ha durata di 3 giorni e produce 3 crediti.

Service Capability con i seguenti moduli formativi e relative certificazioni:

- Service Offerings and Agreements
- Release, Control and Validation
- Operational Support and Analysis
- Planning, Protection and Optimization.

Ognuno di questi moduli ha durata di 5 giorni e produce 4 crediti.
I singoli corsi saranno inseriti in calendario esplicitando in maniera chiara il contenuto e la relativa certificazione.

Ogni corso fornisce infatti le competenze necessarie per sostenere il corrispondente esame di certificazione e si conclude con lo svolgimento dell'esame stesso.

Agenda





La durata e i contenuti variano a seconda dello specifico modulo.

Obiettivi

Acquisire – per ogni modulo - un buon livello di conoscenza su specifici aspetti della metodologia ITIL ed una preparazione adeguata a superare il relativo esame di certificazione.

Destinatari

Quanti hanno già conseguito la certificazione ITIL® v3 Foundation e che desiderano perseguire il percorso di certificazione ITIL.

Prerequisiti

Aver superato l'esame ITIL v3 Foundation" (solo nel caso si desideri affrontare l'esame di certificazione per il modulo di interesse).



ITIL® V3 Managing Across Lifecycle

Il corso completa il processo di certificazione ITIL® di livello intermediate e consente – producendo 5 crediti - di accedere all'esame di certificazione di livello Expert se durante il percorso si sono conseguiti:

- certificazione "ITIL v3 Foundation" (o anche versioni precedenti, opportunamente aggiornate)
- almeno 17 crediti a livello "ITIL v3 Intermediate"
- conoscenza bilanciata di tutte le componenti di ITIL V3 Service Lifecycle.

Il corso consente di completare le competenze necessarie per sostenere l'esame di certificazione e si conclude con l'esame "ITIL v3 Expert".

Agenda





Introduzione alle problematiche gestionali e di business relative all'IT Service Management:

- il controllo a catena chiusa e a catena aperta, quando e dove utilizzarli.

Gestione della pianificazione e implementazione dell' IT Service Management:

- il ciclo "Plan, Do, Check, Act"
- politiche di implementazione
- dirigere, controllare, valutare
- comunicazione, coordinamento, controllo.

Gestione del cambiamento strategico:

- creazione del valore e componenti critiche di successo
- benefici tangibili e intangibili
- gestione della domanda, portafoglio e catalogo servizi.

Risk Management:

- modelli per una efficace valutazione, analisi e identificazione dei rischi
- analisi del rischio in base ai fattori critici di successo.

Comprensione delle sfide organizzative:

- maturità organizzativa e struttura organizzativa
- modelli di gestione
- transizione organizzativa.

Valutazione del servizio:

- tecniche di misura, metriche e monitoraggio
- valore del benchmarking
- valutazione del portafoglio servizi e azioni correttive.

Comprensione del Complementary Industry Guidance.

Il corso include la preparazione e l'esame di certificazione.

Obiettivi

Acquisire, testare e validare con l'esame finale la conoscenza completa e bilanciata di tutti i contenuti di ITIL v3.

Destinatari

Quanti desiderano perseguire la certificazione ITIL® v3 Expert o ITIL® v3 Master in IT Service Management.

Prerequisiti

Aver superato l'esame ITIL v3 Foundation" e un numero sufficiente di crediti nel percorso Intermediate.

COBIT® 5

COBIT (*Control Objectives for Information and related Technology*) è un modello creato nel 1992 dall'associazione americana degli auditor dei sistemi informativi e dal IT Governance Institute (ITGI) per consentire la gestione dell'ICT. COBIT ha raggiunto lo statuto di norma internazionalmente riconosciuta e l'Unione Europea ha indicato COBIT come uno dei tre standard utilizzabili per garantire il controllo e governo dell'IT. COBIT non è solo progettato per gli Utenti e gli Auditor ma principalmente per il Management. È una guida per i manager ed i responsabili dei processi aziendali al governo dell'IT al fine di fornire le corrette informazioni di cui una azienda ha bisogno, sempre considerando gli obiettivi di Business. Il modello divide il controllo della funzione IT in quattro domini: Pianificazione e Organizzazione, Acquisizione e Implementazione, Erogazione ed Assistenza, Monitoraggio e Valutazione. Nei quattro domini sono collocati 34 processi, ai quali fanno capo 210 obiettivi di controllo.

Agenda (2 giorni)

Introduzione al modello COBIT.

La IT Governance e I suoi obiettivi.

COBIT and IT Governance.

COBIT:

- definizioni
- risorse
- processi
- metriche.

La Valutazione del Modello di Maturità e le tecniche di indagine.

Il Current Maturity Model (CMM).

Decidere le priorità e orientare gli investimenti.

Simulazioni del test di certificazione.

Obiettivi

Fornire le competenze sul modello e sulla sua implementazione.

Destinatari

Direttori e Responsabili IT, Responsabili della Sicurezza, Responsabili di progetti informatici e di servizi IT, Responsabili Qualità.

Prerequisiti

È preferibile avere una conoscenza di base sui processi IT.



Cloud Computing

Il corso ha lo scopo di introdurre il concetto di Cloud Computing, partendo dalla descrizione dei singoli elementi che compongono una moderna architettura IT, e trattando tutti i sistemi e le applicazioni che consentono la realizzazione di un Centro Elaborazione Dati Evoluto e la sua virtualizzazione.

Agenda (3 giorni)



Le basi sui Sistemi Operativi:

- hardware (dal Mainframe ai Server su Rack)
- software (dal VMS a Linux Enterprise)
- Unix, cenni storici
- i principali S.O. Unix (AIX, HPUX, Solaris, Linux), Windows Server 2008
- architettura del S.O.
- utenze, Processi, Dischi e Filesystem
- comandi shell base
- concetti base sul Networking
- concetti di Sicurezza ICT (Firewall, IDS, IPS, VPN)
- esercitazione sugli argomenti trattati (Installazione e configurazione di un S.O. Unix).

Infrastrutture IT:

- il Concetto di Architettura IT
- il CED (Centro Elaborazione DATI)
- il Concetto di Server e le sue applicazioni
- il Cluster
- lo Storage (HDD, Array, SAN, NAS, LVM, iSCSI, FC)
- Business Continuity & Disaster Recovery
- esercitazione sugli argomenti trattati (Disegno di un Architettura).

Dall'Infrastruttura Fisica a quella Virtuale:

- teoria della Virtualizzazione
- il concetto di Hypervisor
- la Macchina Virtuale
- Virtual Appliance
- principali software di Virtualizzazione (VMWare, CITRIX, RedHat)
- la Sicurezza degli Ambienti Virtuali
- esercitazione (Installazione di un Host, Creazione di VM, Installazione di un S.O. su VM).

Cloud Computing:

- definizioni
- IaaS, PaaS e SaaS
- Private Cloud, Public Cloud, Service Provider
- la Sicurezza nel Cloud
- software di Cloud Computing
- struttura di un Data Center Evoluto
- esercitazione (Test via VPN di un'infrastruttura Cloud).

Esemplificazioni.

Obiettivi

Conoscere un'architettura Cloud e saperne definire le specifiche.

Destinatari

Responsabili ICT, Amministratori di rete e Responsabili e tecnici di Data Center.

Prerequisiti

Sono richieste conoscenze di base di hardware e software di sistemi informatici.



Data Center: Storage Networking e Server Virtualization

Il corso affrontata le nuove tematiche del Data Center che è l'ambito in cui si sono verificate le più significative evoluzioni tecnologiche a seguito delle esigenze di grandi prestazioni e elevata affidabilità: lo Storage Networking e la virtualizzazione dei Server. Il corso tratta anche il recente standard FCoE, la convergenza di Fiber Channel e Ethernet, i nuovi draft IEEE che ottimizzano l'accesso alla rete da parte delle Virtual Machines (VM). Per la Virtualizzazione, sono illustrate le soluzioni proposte dai principali vendor del mercato: Microsoft e VMware. Il seminario, fornisce informazioni utili a chi deve decidere quale sia la soluzione di virtualizzazione migliore per la propria infrastruttura.

Agenda (3 giorni)



10, 40 e 100 Gigabit Ethernet.

Concetti di Storage e Storage Networking. Architetture di Storage Networking.

Protocolli di Storage Networking.

Caratteristiche e funzioni di Fiber Channel:

- topologie del Fiber Channel
- Switched Fabric: link aggregation e routing (FSPF)
- Classi di Servizio e Flow Control
- Virtual Fabric o VSAN, zoning.

Convergenza delle tecnologie di rete per il Data Center e FCoE (Fiber Channel over Ethernet).

Il cablaggio all'interno dei Data Center e i nuovi sistemi di terminazione delle fibre ottiche in termini di flessibilità per i frequenti Move-and-Change.

Business Continuity e Disaster Recovery: replica sincrona o asincrona e impatti sulla progettazione della rete locale e geografica.

La virtualizzazione: benefici e flessibilità.

Progettare soluzioni di Virtualizzazione nei Data Center.

La soluzione Microsoft:

- pianificare servizi di virtulizzazione quali Hyper-V, RDS, MED-V e APP-V
- Integrate System Center Suite nell'infrastruttura di virtualizzazione per fornire una strategia di gestione end-to-end.

La soluzione VMware:

- ESX/ESXi Host Design
- vSphere Virtual Datacenter Design
- Best practices per vCenter Server, database, cluster e resource pool design
- vSphere Network Design
- vSphere Storage Design.

Virtual Machine Design.

Come convertire e distribuire le macchine virtuali.

Soluzioni enterprise di storage a supporto delle infrastrutture di virtualizzazione.

Soluzioni di virtualizzazione ad alta disponibilità.

Strategie di backup e disaster recovery.

Obiettivi

Fornire competenze, metodologie, criteri e l'approccio per la progettazione di un Data Center virtualizzato.

Destinatari

Responsabili di Sistemi Informativi, Progettisti e Amministratori di Rete, Tecnici di Supporto, Supervisori di Sicurezza, Security Specialist, Security Manager.

Prerequisiti

Conoscenza di base di Sistemi Informativi, TCP/IP, routing, LAN, Switching e Spanning Tree.



Nuove Architetture per Data Centre nell'approccio Cisco Systems

Oggi molte imprese sono impegnate nel consolidamento e nella virtualizzazione delle risorse per trasformare i propri data center. Sebbene questo sia un approccio corretto per ottimizzare le tecnologie esistenti ed eliminare i silos operativi, si tratta solo di un punto di partenza. Le aziende dovrebbero avere una visione più ampia e guardare alle architetture dei data center in modo innovativo per ottenere nuovi livelli di efficienza, velocità di risposta e affidabilità.
Cisco Data Center 3.0 costituisce una efficace strategia per ottenere tali risultati: con un approccio network centrico, Data Center 3.0 consente alle aziende di ridurre le inefficienze ed i relativi costi e aumentare la flessibilità dei servizi di molti data center, in particolare quelli che si sono evoluti con architetture scarsamente strutturate e basate sul modello "un'applicazione, un server". Applicando al data center principi validi nel mondo Internet, le imprese possono automatizzare la distribuzione di risorse virtualizzate, rendendole disponibili a chiunque ne abbia bisogno e in qualsiasi momento.
Nel breve termine ciò significa maggior efficienza, velocità di risposta e affidabilità per l'infrastruttura del data center, permettendo maggiore crescita e competitività dell'azienda. Inoltre la strategia Cisco consente di sviluppare una solida base per implementare un'architettura virtualizzata e network-based in grado di soddisfare le necessità future delle aziende. Gli argomenti illustrati durante il corso saranno affiancate da attività di laboratorio durante le quali i partecipanti avranno modo di mettere in pratica quanto appreso.

Agenda (2 giorni)



Introduzione all'architettura Cisco Unified Computing.

Identificazione della soluzione Cisco Unified Computing.

Architettuta dei server.

Cisco Unifiend Computing System.

Componenti dell'architettura Cisco UCS.

Gestione della soluzione Cisco Unified Computnig System:

- UCSM.

Connettività in Cisco UCS.

Alta affidabilità in Cisco UCS.

Elementi di Design per Cisco Unified Computing.

Deployment Model in architettura Cisco UCS.

Obiettivi

Fornire competenze, metodologie e criteri e per la gestione del DataCenter attraverso la tecnologia Unified Compunting (UCS) di Cisco.

Destinatari

Responsabili ICT, Amministratori di rete e Responsabili e tecnici di Data Center.

Prerequisiti

Conoscenza di base dei Sistemi Informativi, TCP/IP, Sistema operativo Windows.



Progettazione e configurazione di soluzioni Cisco Unified Computing

Il corso è incentrato sull'implementazione e la gestione pratica della piattaforma Cisco Unified Computing System (UCS). Sono fornite le competenze per installare, configurare, gestire blade server Cisco UCS B-Series e server rack-mount C-Series. Verrà illustrato il consolidamento networking per la connetticità LAN e SAN dei server e la capacità della piattaforma Cisco UCS di virtualizzare le proprietà dei server al fine di abilitare e sfruttare la mobilità dei profili dei server fra i server fisici.

Agenda (3 giorni)

Introduzione all'architettura Cisco Unified Computing.

Iinstallazione e upgrading dei server UCS B-Series e C-Series.

Introduzione e gestione Cisco ICM.

Cisco UCS B-Series Hardware Overview.

Cisco UCS B-Series Configurazione.

Gestione della soluzione Cisco Unified Computnig System:

- UCSM
- LAN Connectivity
- SAN Connectivity.

Obiettivi

Fornire le competenze per l'implementazione e la gestione della piattaforma Unified Compunting (UCS) di Cisco.

Destinatari

Responsabili ICT, Amministratori di rete e Responsabili e tecnici di Data Center.

Prerequisiti

Conoscenza di base dei Sistemi Informativi e networking.



Virtualizzare con VMware: Progetto e Implementazioni

Vmware vSphere, la piattaforma di virtualizzazione per la creazione di infrastrutture cloud leader del settore, fornisce i massimi livelli di disponibilità e reattività e consente agli utenti di eseguire applicazioni business critical in tutta sicurezza, rispondendo più rapidamente alle esigenze aziendali.
vSphere aiuta le organizzazioni ad erogare i servizi IT in maniera più efficiente eliminando gli investimenti non necessari e riducendo costi e complessità associati alla gestione e manutenzione dell'infrastruttura IT.
Con l'adozione di VMware vSphere i clienti possono ridurre gli investimenti di capitale e le spese operative di ciascuna applicazione, abbattendo il costo complessivo di gestione delle applicazioni aziendali.
La virtualizzazione elimina la proliferazione dei server eseguendo le applicazioni all'interno di macchine virtuali installate su un numero inferiore di server e con un utilizzo più efficiente delle risorse di rete e storage. Le organizzazioni che utilizzano la virtualizzazione possono conseguire rapporti di consolidamento per singolo server elevatissimi grazie a straordinarie funzionalità di gestione della memoria e ottimizzazione dinamica. VMware vSphere™ riduce la complessità di gestione dell'hardware mediante la virtualizzazione totale di server, storage e hardware di rete.
Gli argomenti illustrati durante il corso saranno affiancati da attività di laboratorio durante le quali i partecipanti avranno modo di testare alcune funzionalità di Vmware vSphere.

Agenda (3 giorni)



Progettare soluzioni di Virtualizzazione nei Data Center.

La soluzione VMware vSphere:

- introduzione alla virtualizzazione con VMware
- installazione e gestione dell'Hypervisor vSphere ESXi
- VMware vCenter – installazione e gestione del DataCenter
- networking in ambiente virtuale
  - Configurazione dello switch virtuale (vSwitch) delle connessioni di rete e dei gruppi di porte
  - Gestione dei vitual switch con vCenter
- gestione dello Storage e allocazione dello spazio per le Virtual Machine
- creazione e gestione delle Virtual Machine
- Virtual Machine Management
  - Clone
  - Template
  - Gestione delle risorse
- gestione delle funzionalità avanzate - vMotion, HA, FT e DRS.

Esempi pratici sulla piattaforma Vmware vSphere.

Obiettivi

Fornire competenze, metodologie e criteri per la gestione di un DataCenter in ambiente virtualizzato.

Destinatari

Responsabili ICT, Amministratori di rete e Responsabili e tecnici di Data Center.

Prerequisiti

Conoscenza di base dei Sistemi Informativi, basi sul networking, gestione base dei sistemi operativi.



Excel Avanzato: importazione, analisi e reporting

In ambito aziendale e professionale, ottenere analisi e reporting immediati e aderenti alle proprie esigenze è spesso difficile e dispendioso. Molte volte si hanno informazioni sparse e distribuite su diverse piattaforme. Raccogliere dati, trasformare i dati in informazioni utili e utilizzare le informazioni per fornire conoscenze, sono possibili anche grazie all'uso avanzato di Excel che mette a disposizione strumenti per importare dati provenienti da una qualsiasi fonte e per costruire report sintetici ed efficaci, fino a ad essere considerati front end del sistema di Business Intelligence aziendale.

Agenda (3 giorni)



Panoramica nuovo ambiente di lavoro di Excel:

- le Schede, i Gruppi, la Barra di Accesso Rapido, l'ambiente di Lavoro di Excel.

Panoramica sulle funzionalità avanzate di Microsoft Office Excel.

Vincoli sui dati:

- convalidare i dati; il messaggio di input; il messaggio di output.

Analisi in dettaglio delle formule:

- ricerca e riferimento; testo; statistiche; matematiche e trigonometriche; logiche.

Le formule matrici:

- introduzione alle formule matrici.

Gestire i dati:

- convalidare i dati.

Caricare dati da fonti esterne:

- il gruppo Carica dati esterni; importare dati da un file di testo; importare dati da un file Access;
- importare dati dal Web
- importare dati da altre origini (XML, Microsoft query, SQL Server, etc.).

Ordinare i dati:

- i filtri semplici; i filtri avanzati.

Analizzare i dati:

- i Subtotali
- le tabelle pivot
- i grafici pivot
- gli scenari
- la ricerca obiettivo.

Le Macro:

- registrare una macro; punto di memorizzazione; riferimento relativo; eseguire una macro; modificare una macro; assegnare una combinazione di tasti ad una macro; assegnare un pulsante ad una macro.

I Grafici:

- la creazione ed il salvataggio di grafici personalizzati: l'aggiornamento automatico, la creazione di grafici rolling; l'inserimento di testo e di tabelle nel grafico.

I Report:

- gli strumenti a disposizione; report statici; report dinamici
- report multidimensionali

Obiettivi

Alla fine del corso i partecipanti saranno in grado di importare i dati presenti su altre piattaforme e di realizzare grafici e report direzionali efficaci.

Destinatari

Tutti i livelli aziendali.

Prerequisiti

Conoscenza di Excel a livello intermedio.



Excel VBA

Excel VBA (Visual Basic for Applications) permette di creare automazioni, sviluppare nuove funzionalità ed avere una marcia in più nell'utilizzo di Microsoft Excel. VBA opera sugli oggetti presenti in Excel come cartelle e fogli di lavoro, singole celle, range, righe e colonne, ma anche grafici, tabelle, formule e tutte le altre funzionalità di Excel.
Il corso fornisce le nozioni di base per essere subito operativi, inoltre vengono riportati esempi pratici che permettono un immediato riscontro con i concetti appresi.

Agenda (2 giorni)



Breve riepilogo interfaccia.

Proprietà celle e formattazione.

I tipi di dati e calcoli con le date.

Le funzioni incorporate.

Filtri e gestione dei dati.

Tabelle Pivot.

Strumenti di analisi e convalida dei dati.

Introduzione al VBA e ambiente di sviluppo.

La sintassi Visual Basic.

Operatori e variabili.

Proprietà Eventi e Metodi.

Debug e gestione degli errori.

Il registratore di Macro.

Creazione di funzioni personalizzate.

Gli oggetti di Excel.

Interazione fogli di lavoro da VBA.

Automatizzazione fogli di lavoro.

Creazione di procedure.

Personalizzazione dell’ambiente.

Esercitazioni.

Obiettivi

Fornire conoscenze di base per mettere in condizione di operare con Excel VBA.

Destinatari

Tutti i livelli aziendali.

Prerequisiti

Conoscenza di Excel a livello intermedio.



Programming in C#

C# è uno dei linguaggi che fa parte della suite di sviluppo Visual Studio 2012. Le caratteristiche di linguaggio di programmazione orientato agli oggetti: ereditarietà, polimorfismo e overloading non sono più prerogative solo di Java e C++.
Il corso introduce con gradualità i concetti fondamentali della programmazione C# (strutture di controllo, procedure, array, programmazione orientata agli oggetti, interfacce utente grafiche), offrendo al tempo stesso una panoramica ampia e articolata del linguaggio, dell'ambiente integrato di sviluppo Visual Studio 2012 e delle caratteristiche di .NET Framework 4.5.
Il corso valido per la preparazione all'esame di certificazione 70-483 e il conseguimento della certificazione MCSD.

Agenda (5 giorni)





Review of C# Syntax:

- overview of Writing Applications using C#
- Datatypes, Operators, and Expressions
- C# Programming Language Constructs.

Creating Methods, Handling Exceptions, and Monitoring Applications:

- creating and Invoking Methods
- creating Overloaded Methods and Using Optional and Output Parameters
- Handling Exceptions
- Monitoring Applications.

Developing the Code for a Graphical Application:

- implementing Structs and Enums
- Organizing Data into Collections
- Handling Events.

Creating Classes and Implementing Type-safe Collections:

- creating Classes
- defining and Implementing Interfaces
- implementing Type-safe Collections.

Creating a Class Hierarchy by Using Inheritance:

- creating Class Hierarchies
- extending .NET Framework Classes
- creating Generic Types.

Reading and Writing Local Data:

- reading and Writing Files
- Serializing and Deserializing Data
- performing I/O Using Streams.

Accessing a Database:

- creating and Using Entity Data Models
- querying Data by Using LINQ
- updating Data by Using LINQ.

Accessing Remote Data:

- accessing Data Across the Web
- accessing Data in the Cloud.

Designing the User Interface for a Graphical Application:

- using XAML to Design a User Interface
- binding Controls to Data
- styling a User Interface.

Improving Application Performance and Responsiveness:

- Implementing Multitasking by using Tasks and Lambda Expressions
- performing Operations Asynchronously
- synchronizing Concurrent Access to Data.

Integrating with Unmanaged Code:

- creating and Using Dynamic Objects
- managing the Lifetime of Objects and Controlling Unmanaged Resources.

Creating Reusable Types and Assemblies:

- examining Object Metadata
- creating and Using Custom Attributes
- generating Managed Code
- versioning, Signing and Deploying Assemblies.

Encrypting and Decrypting Data:

- implementing Symmetric Encryption
- implementing Asymmetric Encryption.

Obiettivi

Fornire le conoscenze e le competenze necessarie per creare applicazioni C# utilizzando Visual Basic 2012.

Destinatari

Programmatori e sviluppatori di applicazioni.

Prerequisiti

Conoscenza delle basi di programmazione, dell'ambiente di sviluppo Visual Studio (IDE) e del linguaggio C#.



Strumenti per il WEB: Applicazioni ASP

ASP è un linguaggio di programmazione lato server utile per la realizzazione di applicazioni web oriented, in grado di consentire interazione client-server e di produrre dinamicamente contenuti web per siti di e-commerce, blog, gallerie fotografiche, newsletter etc.

Agenda (3 giorni)



Introduzione al VBScript.

Introduzione alle ASP.

Utilizzo degli oggetti.

Costrutti utilizzabili nella pagine ASP.

ASP e i Database.

Comunicazione con l'utente.

Mantenere dati persistenti nel web.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di realizzare pagine web dinamiche, consentire l'interazione tra i contenuti web e un database, gestire salvataggio e gestione dei dati provenienti da una form.

Destinatari

Progettisti software, programmatori, personale tecnico di supporto.

Prerequisiti

Conoscenza base del linguaggio html e dei fogli di stile css.

Developing ASP.NET MVC 4 Web Applications

La piattaforma ASP.NET è indispensabile per chi vuole progettare siti complessi, dinamici, che offrano interazione con l'utente (commercio elettronico, portali dinamici, Forum e sistemi di gestione dei contenuti). In questo corso gli allievi impareranno a sviluppare applicazioni di tipo avanzato (ASP.NET MVC e Web Forms) utilizzando gli strumenti e le tecnologie .NET Framework 4.
ASP.NET MVC viene introdotto e confrontato con le Web Forms in modo tale che l'allievo possa scegliere la modalità a lui più congeniale. **Corso valido per la preparazione all'esame di certificazione 70-486 e il conseguimento della certificazione MCSD**.

Agenda (5 giorni)





Exploring ASP.NET MVC 4:
- overview of Microsoft Web Technologies
- overview of ASP.NET 4.5
- introduction to ASP.NET MVC 4.

Designing ASP.NET MVC 4 Web Applications:
- planning in the Project Design Phase
- designing Models, Controllers, and Views.

Developing ASP.NET MVC 4 Models:
- creating MVC Models
- working with Data.

Developing ASP.NET MVC 4 Controllers:
- writing Controllers and Actions
- writing Action Filters.

Developing ASP.NET MVC 4 Views:
- creating Views with Razor Syntax
- using HTML Helpers
- reusing Code in Views.

Testing and Debugging ASP.NET MVC 4 Web Applications:
- Unit Testing MVC Components
- implementing an Exception Handling Strategy.

Structuring ASP.NET MVC 4 Web Applications:
- analyzing Information Architecture
- configuring Routes
- creating a Navigation Structure.

Applying Styles to ASP.NET MVC 4 Web Applications:
- using Template Views
- applying CSS to an MVC Application
- creating an Adaptive User Interface.

Building Responsive Pages in ASP.NET MVC 4 Web Applications:
- using AJAX and Partial Page Updates
- implementing a Caching Strategy.

Using JavaScript and jQuery for Responsive MVC 4 Web Applications:
- rendering and Running JavaScript Code
- using jQuery and jQueryUI.

Controlling Access to ASP.NET MVC 4 Web Applications:
- implementing Authentication and Authorization
- assigning Roles and Membership.

Building a Resilient ASP.NET MVC 4 Web Application:
- developing Secure Sites
- state Management.

Developing ASP.NET MVC 4 Web Applications

Using Windows Azure Web Services in ASP.NET MVC 4 Web Applications:
- introduction to Windows Azure
- designing and Writing Windows Azure Services
- consuming Windows Azure Services in a Web Application.
- Applying CSS, Skins, and Themes.

Implementing Web APIs in ASP.NET MVC 4 Web Applications:
- developing a Web API
- calling a Web API from Mobile and Web Applications.

Handling Requests in ASP.NET MVC 4 Web Applications:
- using HTTP Modules and HTTP Handlers
- using Web Sockets.

Deploying ASP.NET MVC 4 Web Applications:
- deploying Web Applications
- deploying MVC 4 Applications.

Obiettivi

Il corso si propone di trasmettere ai partecipanti le conoscenze e le competenze necessarie per:
- applicare le tecniche più appropriate nella progettazione di applicazioni Web
- sviluppare modelli, controller e viste MVC
- ottimizzare la progettazione di applicazioni Web ai fini delle ricerca attraverso i motori di ricerca
- scrivere codice server-side per le Web Forms
- rendere sicura una applicazione Web
- applicare Master Pages e CSS
- sviluppare servizi Windows Azure e script JavaScript client-side
- eseguire test, debug e troubleshooting delle applicazioni.

Destinatari

Programmatori e sviluppatori di applicazioni.

Prerequisiti

Conoscenza delle caratteristiche di .NET Framework e dell'utilizzo di Visual Studio. Conoscenza di base di linguaggi di programmazione ad oggetti.



Strumenti per il WEB: Creare animazioni con Adobe Flash CS5.5

Adobe Flash è un software versatile in grado di creare animazioni vettoriali bidimensionali per il web e non solo; consente la gestione di presentazioni multimediali comprensivi di audio e video, la creazione di animazioni e cartoon, la gestione del web advertising e l'elaborazione di prodotti per l'e-learning.

Agenda (3 giorni)



Introduzione all'ambiente di lavoro Adobe Flash CS5.5.

Tutti gli oggetti nativi flash.

Flash e le animazioni.

Flash e il web.

Il linguaggio ActionScript 3.0.

Le condizioni e i Loop.

La grafica.

Importare grafica bitmap esterna e swf secondari.

Importare file di testo e Preload dei dati.

Adobe Flash e la multimedialità.

Animazioni avanzate: drag & drop, sovrapposizione e collisioni di oggetti.

Interazione dati Flash e XML.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare gli strumenti per realizzare presentazioni multimediali con Adobe Flash, gestire contenuti testuali e grafici esterni, audio e video, realizzare preload e creare animazioni avanzate con effetti di drag & drop, sovrapposizioni e collisioni di oggetti.

Destinatari

Grafici, programmatori e tutti coloro che vogliono imparare a realizzare animazioni in Flash.

Prerequisiti

Nessuno.



XML e tecnologie afferenti

XML rappresenta oggi lo standard "de facto" con cui le applicazioni web possono scambiare dati, rappresentare significati e funzioni. XML è ampiamente usato per rappresentare standard di interoperabilità tra applicazioni web (nell'e-learning, nell'e-commerce, etc.) oltre che per riuscire a fornire contenuti fruibili in modo indipendente dai dispositivi usati (pc, palmare, cellulare, etc...). È fondamentale dunque oggi conoscere l'XML per riuscire a comprendere il modo in cui il web si sta evolvendo e rappresentando.

Agenda (3 giorni)



Introduzione al linguaggio XML:

- concetti base di XML, uso e benefici
- Campi applicativi di XML
- XML e il mondo WEB.

La sintassi:

- definizione della grammatica: DTD
- l'evoluzione della grammatica: introduzione all'XML Schema.

La pubblicazione dei documenti XML:

- XSLT: il linguaggio per la presentazione
- gli scenari delle presentazioni: HTML,WML e SVG
- cenni sulla pubblicazione con XML-FO: generazione di documenti PDF.

XML dal lato della programmazione:

- il parser XML: come costruire l'albero del documento
- l'interfaccia del DOM: Document Object Model
- introduzione al SAX: Simple API for XML.

Uno sguardo al futuro:

- evoluzione del linguaggio: Xlink, Xpointer.

Obiettivi

Comprendere la sintassi e la semantica del linguaggio XML.
Comprendere la sintassi e la semantica del linguaggio DTD/Schema.
Pubblicare un documento XML.

Destinatari

Sviluppatori di applicazioni, analisti e programmatori, responsabili coinvolti nello sviluppo di applicazioni in XML, committenti di applicazioni.

Prerequisiti

Conoscenze nell'utilizzo della rete Internet e del Web; buona conoscenza di HTML; conoscenze base programmazione Object Oriented e linguaggi di scripting.

La programmazione Object Oriented in Java

Il corso illustra le caratteristiche di Java, enfatizzando la metodologia di sviluppo orientata agli oggetti. In particolare, vengono presentate le caratteristiche sintattico semantiche di Java, aggiornate alla versione del JDK 6.0, la metodologia di progettazione e le differenze con gli altri linguaggi di programmazione come il C++ e C#. A completamento della trattazione teorica, sono previste numerose esercitazioni.

Agenda (4 giorni)



Introduzione all'architettura JEE.

Introduzione al linguaggio Java.

Costrutti di base del linguaggio:

- tipi di dati; classi, metodi e costruttori
- ereditarietà e polimorfismo
- Generics, Enums, Autoboxing e unboxing, ecc.

La programmazione orientata a oggetti in Java:

- implementazione delle classe e istanziazione degli oggetti
- relazioni fra le classi: associazione, aggregazione, composizione, realizzazione
- rappresentazione della dinamica fra le istanze delle classi con i diagrammi di sequenza UML.

Applicazioni Java e caratteristiche del linguaggio:

- Package e la modularizzazione dei programmi Java
- Inner Class
- gestione delle eccezioni
- annotazioni
- introduzione alla programmazione multithread
- cenni alle "Applet" e alle API AWT
- documentazione di progetto.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze teoriche e pratiche su Java e sulla relativa metodologia di progettazione, aggiornate alla versione del JDK 6.0.

Destinatari

Sviluppatori di applicazioni, analisti e programmatori, responsabili coinvolti nello sviluppo di applicazioni.

Prerequisiti

Nessuno.



Web programming e usabilità con PHP e MySQL

II mondo dei servizi web è sempre più il terreno di battaglia sul quale si giocano sfide decisive per il successo degli Operatori: oggi, infatti, il Cliente è divenuto più sensibile anche al “modo” in cui i servizi possono essere offerti. L’Usabilità ha assunto un ruolo strategico nella progettazione dei servizi e delle applicazioni divenendo linea guida obbligatoria nella progettazione di applicazioni Web.
Il PHP è un linguaggio di scripting di tipo “server side” utilizzato per realizzare applicazioni web complesse. È un linguaggio multipiattaforma ed open source con molte funzionalità native, ideale per essere impiegato insieme con MySql, un database server utilizzato nell’ambito di applicazioni professionali.

Agenda (3 giorni)



Introduzione ai principi di Usabilità, definizioni e generalità:

- vantaggi, diffidenze e problemi
- confronto tra ergonomia e usabilità dei sistemi informatici.

Usabilità delle interfacce Software:

- capire: la psicologia cognitiva e lo sforzo cognitivo, la memoria e I 2 golfi dell’Usabilità
- realizzare: obiettivi del progetto, garantire la visibilità, proporre inviti e vincoli d’uso, fornire un adeguato modello concettuale, semplificare i compiti, restituire feedback e gestire l’errore
- valutare e misurare: test di usabilità condotti con o senza il contributo degli utenti, basati su metodi di survey (questionari) o con l’ausilio di strumenti automatici.

Il colore e l’usabilità, la ruota dei colori, accostamenti cromatici schemi cromatici.

Esempi: saranno esaminati alcuni siti allo scopo di valutare il livello di usabilità e lo sforzo cognitivo.

Come sviluppare un sito web e la sua usabilità con il PHP.

La sintassi: variabili, strutture if, for, while, switch.

Funzionalità per mantenere lo stato delle variabili: $_GET, $_POST, $_SESSION, $_COOKIES.

Inviare email-newsletter tramite PHP.

Introduzione alle funzioni utente e le funzioni native e per la manipolazione delle stringhe.

Accesso e manipolazione di file esterni.

L’accesso a DB esterni MYSQL.

Interrogazioni dati tramite SQL.

Query di selezione e restituzione di dati all’applicazione client.

Esempi di realizzazione di applicazioni web che verifichino i requisiti minimi di usabilità.

Obiettivi

Illustrare i principi dell’usabilità delle applicazioni informatiche, le metodologie e le fasi dello sviluppo delle applicazioni web usabili e come svilupparle in PHP e MySql.

Destinatari

Sviluppatori di applicazioni web.

Prerequisiti

Conoscenza del linguaggio HTML 4.01/XHTML e dei fogli stile CSS.

Gang of Four Design Patterns

Nell'ingegneria del Software, un design pattern può essere definito come "la descrizione di una soluzione provata ad un problema ricorrente in un determinato contesto".
In pratica un design pattern è una regola che esprime una relazione tra un contesto, un problema ed una soluzione.
Dal 1990 al 1992 la famosa Gang of Four (Gamma, Helm, Johnson, Vlissides) incominciò la stesura di un catalogo di pattern, considerato il riferimento per tutti gli altri patterns.

Agenda (3 giorni)

Introduzione ai Design Patterns.

Design Pattern Creazionali:

- Abstract Factory
- Builder
- Factory Method
- Prototype
- Singleton.

Design Pattern Strutturali:

- Adapter
- Bridge
- Composite
- Decorator
- Facade
- Flyweight
- Proxy.

Design Pattern Comportamentali:

- Chain of Responsibility
- Command
- Interpreter
- Iterator
- Mediator
- Memento
- Observer
- State
- Strategy
- Template Method
- Visitor.

Obiettivi

Al termine del corso i partecipanti saranno in grado di riconoscere un problema ricorrente e di applicare il relativo pattern.

Destinatari

Analisti e Progettisti di applicazioni software; Responsabili di progetti software.

Prerequisiti

Competenze di Object Oriented (ereditarietà, polimorfismo, incapsulamento) e dimestichezza con il linguaggio Java (costrutti di classi astratte e interfacce). Completano il profilo ideale nozioni di UML.



Lo sviluppo di applicazioni di business con gli Enterprise Java Bean 3.1

Il nuovo modello degli Enterprise Java Bean 3.1 è stato introdotto con la piattaforma Java Enterprise Edition 6, per lo sviluppo di applicazioni di business a livello enterprise.
Nel corso, insieme allo sviluppo dei vari tipi di Enterprise Java Bean, si affrontano gli aspetti legati alla transazionalità delle operazioni, alla sicurezza e alla gestione della persistenza. Infine, si illustra come esporre le operazioni degli Enterprise Java Bean attraverso i web services XML per inserire i componenti di business nel contesto della Service-Oriented Architecture (SOA).

Agenda (4 giorni)



Introduzione:

- caratteristiche di un'applicazione di business
- il concetto di componente e sue caratteristiche
- cos'è un'architettura basata su componenti
- introduzione a Java Enterprise Edition.

Introduzione agli Enterprise Java Bean (EJB) 3.1:

- perché gli EJB
- il modello degli EJB 3.1
- cos'è un application server e un EJB container
- tipologie di EJB: Session Bean (stateless, stateful), Singleton Session Bean, Message-Driven Bean
- differenze fra gli EJB 3.1, EJB3.0 e gli EJB 2.x.

Tecnologie per sviluppare gli EJB 3.1:

- Java annotation
- Java Naming & Directory Interface (JNDI)
- Java Database Connectivity (JDBC)
- Java RMI/IIOP
- Java Persistence (JPA).

I Session Bean.

Singleton Session Bean.

I Bean e la persistenza.

I message-driven bean.

La gestione delle transazioni con gli EJB.

La sicurezza degli EJB.

Il Timer Service con gli EJB 3.1.

Esposizione delle operazioni degli EJB con i web services XML.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce conoscenze teoriche e pratiche sulle caratteristiche di un'applicazione di business, sulle architetture basate su componenti e sugli Enterprise Java Bean e le relative tecnologie di sviluppo per EJB3.1.

Destinatari

Sviluppatori di applicazioni per l'integrazione di applicazioni eterogenee distribuite su multipiattaforme, responsabili dello sviluppo di applicazioni.

Prerequisiti

Conoscenza del linguaggio Java.



Sharepoint 2010 Business Intelligence

Nel corso si analizzerà l'utilizzo di Sharepoint come piattaforma di Business intelligence. In particolare si comprenderà come configurare ed usare Excel Services, Reporting Services, Analysis Service, Performance Point e PowerPivot. A completamento della trattazione teorica, sono previste numerose esercitazioni.

Agenda (4 giorni)



Sharepoint: introduzione.

Business Intelligence Center.

Definizione di data warehouse e data mart.

Business Connectivity Services.

Analysis Services.

Reporting Services.

Excel Services.

PowerPivot.

Performance Point.

Gestione di dati geospaziali.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze teoriche e pratiche su Business Intelligence Center, Analysis Services, Reporting Services, Excel Services, Business Connectivity Services, Power Pivot, Performance Point e Bing Maps.

Destinatari

Professional interessati alla manipolazione, gestione e archiviazione dati, responsabili e progettisti IT, analisti e programmatori.

Prerequisiti

Nessuno.



Framework Struts

Il Framework Struts è un insieme di classi ed interfacce che costituiscono l'infrastruttura per costruire web application Java EE conformi al design pattern MVC. Questo framework, gestisce tutte le richieste client e smista il flusso applicativo in base alla logica configurata. Si potrebbe definire come la "spina dorsale" di una applicazione che adotta tale framework. Tutta la configurazione dell'applicazione è contenuta all'interno di uno specifico file XML che viene letto in fase di start-up dell'applicazione e definisce le associazioni tra i vari elementi che compongono il Sistema.

Agenda (3 giorni)

Introduzione al Framework Struts e al ruolo che occupa nello scenario dell'architettura Java EE.

Introduzione al modello architetturale e al Pattern Model-View-Controller.

I componenti del Framework e i plugin aggiuntivi.

Internazionalizzazione delle applicazioni Str3uts.

Validazione client side, validazione server side e Jakarta Commons Validator.

Costruzione del layout dell'applicazione con Tiles.

Eccezioni e gestione degli errori.

Obiettivi

Fornire conoscenze teorico pratiche per poter usare il framework Struts.

Destinatari

Sviluppatori di applicazioni WEB, programmatori, responsabili coinvolti nello sviluppo di applicazioni.

Prerequisiti

Conoscenza base della programmazione web in Java (Servlet, JSP, tag libraries).



Il Framework Hibernate

Hibernate è un framework open source per lo sviluppo di applicazioni Java che fornisce un servizio di Object-relational mapping (ORM), ovvero che gestisce la rappresentazione e il mantenimento su database relazionale di un sistema di oggetti Java. L'obiettivo principale di Hibernate è quello di liberare lo sviluppatore dall'intero lavoro relativo alla persistenza dei dati.

Agenda (3 giorni)

Persistenza di oggetti Java su database relazionali:

- il problema dell’impedance mismatch, object/relational mapping, possibili soluzioni.

Introduzione a Hibernate

- breve descrizione dell’architettura
- componenti fondamentali e configurazione.

Mapping delle classi persistenti:

- modello di dominio degli oggetti
- file di mapping XML
- identità degli oggetti e granularità
- mapping delle relazioni di ereditarietà e delle associazioni.

Operazioni su oggetti persistenti:

- ciclo di vita
- operazioni CRUD
- caratteristiche avanzate
- linguaggi di query.

Strategie di gestione delle transazioni, della concorrenza e meccanismo di caching.

Mapping avanzato:

- CustomTypes
- mapping di Collections
- relazioni e associazioni polimorfiche.

Performance tuning:

- ottimizzazione delle query e funzionalità avanzate dei linguaggi di query.

Hibernate toolset:

- panoramica sugli strumenti (open-source) a supporto dello sviluppo.

Obiettivi

Fornire le basi per la progettazione e l’implementazione di applicazioni basate su Hibernate per la persistenza di oggetti Java su database relazionali. Offrire una panoramica sulle metodologie e gli strumenti più comunemente utilizzati.

Destinatari

Sviluppatori di applicazioni, responsabili e progettisti interessati alla manipolazione, gestione e archiviazione dati, responsabili coinvolti nello sviluppo di applicazioni.

Prerequisiti

Buona conoscenza del linguaggio Java, sufficiente conoscenza del linguaggio SQL. La conoscenza dell’architettura J2EE è un requisito preferenziale non discriminante.



Sviluppo di applicazioni Web con Servlet e JSP

Il corso fornisce le competenze necessarie per sviluppare applicazioni server-side con le Java Servlet e le Java Server Page, tecnologie software che godono dei benefici di robustezza ed economicità offerti dal mondo Java e sono in grado di garantire flessibilità e portabilità alle applicazioni.

Agenda (4 giorni)



L'architettura J2EE.

Introduzione ai web component Java: servlet e Java Server Pages (JSP).

Le servlet:

- caratteristiche e struttura di una servlet
- ciclo di vita di una servlet
- la servlet "Hello World"
- il deployment di una servlet
- il container dei web component: caratteristiche e servizi offerti
- nozioni fondamentali delle API JDBC per l'accesso ai database
- creazione di connessioni a un database nella servlet
- la gestione delle sessioni utente
- la gestione della sicurezza
- utilizzo delle transazioni
- creazione di un pool di connessioni attraverso il servlet container
- ottenere una connessione a un database dal container e rilascio della connessione.

Le Java Server Pages:

- caratteristica di una pagina JSP
- ciclo di vita di una JSP
- elementi di una JSP: direttive, elementi d'azione, scriptlet, oggetti impliciti
- utilizzo di Java Bean all'interno delle JSP
- introduzione ai custom tag
- JSTL 2.0.

Struttura standard di una Java web application: il file WAR.

I filtri per la pre e post-elaborazione di una richiesta.

Realizzazione di un'applicazione web utilizzando i pattern fondamentali:

- Model-View-Controller (MVC)
- Front Controller
- Application Controller
- View Helper.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze sull'architettura J2EE e sui componenti Java Servlet e Java Serve Pages (JPS), e le competenze di base necessarie allo sviluppo di applicazioni server-side.

Destinatari

Sviluppatori di applicazioni WEB, programmatori, responsabili coinvolti nello sviluppo di applicazioni. Responsabili di progetto.

Prerequisiti

Conoscenza del linguaggio Java.



Cloud Computing: Porting e progettazione di applicazioni e servizi

Il corso affronta le nuove tematiche del Cloud Computing che si propone di fornire prestazioni e elevata affidabilità nel settore dei servizi. Il corso si propone di presentare le caratteristiche della tecnologia cloud, le architetture e le soluzioni esistenti. Dopo aver presentato gli strumenti di progettazione offerti in un ambiente cloud, mostrerà come si effettua il porting di un'applicazione o di un servizio già esistente o come si progetta una nuova soluzione.

Agenda (3 giorni)

Introduzione al Cloud Computing:

- astrazione e virtualizzazione
- architettura e funzionalità
- infastructure as service, Platform as Service e Software as Service
- vantaggi e svantaggi.

Uso di piattaforme commerciali:

- Google Web Service
- Amazon Web Service
- Microsoft Cloud Service
- il mercato italiano.

Progettazione di applicazioni e servizi:

- gestione del Cloud
- pianificazione e tuning delle risorse
- gestione della sicurezza
- porting di applicazioni
- Cloud-based Storage
- applicazione servizi per il Mobile.

Obiettivi

Preparare progettisti e manager a realizzare applicazioni e servizi in un contesto cloud.

Destinatari

Progettisti e Manager.

Prerequisiti

Conoscenza di base per la progettazione di applicazioni e servizi.



JBOSS for Administrators

JBoss è un Application Server open source multipiattaforma, che implementa l'intera suite di servizi Java EE, utilizzabile su qualsiasi sistema operativo che supporti Java.
Il corso descrive le attività di installazione di JBoss e il suo utilizzo, oltre che la configurazione e il monitoraggio del server per tutte le attività cui esso è destinato.
I contenuti del corso consentono di acquisire competenze utili al conseguimento della certificazione JBoss Administration.

Agenda (4 giorni)





Installazione e configurazione base di JBoss Enterprise Application Platform:

- risorse hardware e sofware richieste
- installazione del front-end grafico.

Installazione delle applicazioni enterprise in JBoss:

- tecnologie: JBoss EAP, J2/JEE, pacchetti installabili.

Monitoraggio e controllo di JBoss:

- i Tools per monitorare le installazioni JBoss, e la configurazione di questi strumenti e quali informazioni forniscono
- JBoss Operations Network per monitorare e gestire le applicazioni installate nel server di applicazione
- monitoraggio del server di applicazione con Jconsole.

Collegamento a JBoss:

- connessione e accesso alle componenti JBoss
- Java Naming e Directory Interface e Java Messaging Service
- come proteggere le porte di ingresso dagli attacchi di denial-of-service
- applicazioni Web.

Applicazioni di sicurezza con le soluzioni JBoss:

- la sicurezza in ambiente enterprise
- JAAS, LDAP, HTTP/S, certificati SSL.

Applicazioni di risoluzione dei problemi su JBoss:

- strumenti disponibili per favorire la comprensione e per identificare i potenziali problemi di applicazione.

Introduzione al clustering con JBoss:

- installare un'applicazione in cluster.

Introduzione all'ottimizzazione.

Obiettivi

Conoscere l'amministrazione di JBoss, nelle fasi di installazione e utilizzo.
Fornire la preparazione utile al conseguimento della certificazione JBoss Administration.

Destinatari

Amministratori di sistema. Sviluppatori di applicazioni.

Prerequisiti

Esperienza base con l'amministrazione di sistema sui sistemi operativi Windows, Unix o Linux.



Linux, Apache, MySQL, PHP (LAMP)

LAMP è un acronimo che indica una piattaforma per lo sviluppo di applicazioni web che prende il nome dalle iniziali dei componenti software con cui è realizzata (Linux, Apache, MySQL, PHP). La piattaforma LAMP è una delle più utilizzate a livello mondiale: ognuna delle applicazioni dalle quali è composta è predisposta per l'eccellente funzionamento in concomitanza con le altre.

Agenda (3 giorni)

Introduzione al Software Libero e al Sistema Operativo GNU/Linux.

Gestione del sistema:

- il filesystem
- permessi sui file
- gestione degli utenti.

Il Web Server Apache:

- installazione e direttive principali
- moduli aggiuntivi
- configurazione dei Virtual Host.

Il Database MySQL:

- installazione
- creazione e gestione di una base dati
- esercitazioni su queries SQL.

Il linguaggio di scripting PHP:

- creazione di semplici pagine dinamiche
- collegarsi al database MySQL.

Obiettivi

Il corso è pensato per fornire una visione d'insieme della piattaforma LAMP da un punto di vista pratico/operativo. Alla fine del percorso formativo il partecipante è in grado di "mettere su" un server LAMP funzionante.

Destinatari

Amministratori di sistema. Sviluppatori di applicazioni.

Prerequisiti

Conoscenza base del computer e delle tecnologie di rete.

CMS JOOMLA - Base

Un Content Management System (CMS) è un software open source che permette di semplificare la definizione e l'amministrazione dei contenuti di un sito web, svincolando l'amministratore da conoscenze tecniche di programmazione web. La larga diffusione di Joomla è determinata dalla disponibilità dei tantissimi template, sviluppati dalla comunità mondiale, che permettono di estendere le funzionalità dei siti web, ad esempio VirtueMart che consente di aggiungere funzionalità di e-commerce.
Il corso presenta il CMS Joomla, a partire dalla fase di installazione e personalizzazione e mette in grado di realizzare siti web dinamici senza richiedere la modifica o l'inserimento di righe di codice.

Agenda (3 giorni)



Introduzione:

- panoramica sui CMS Open Source e sulle funzionalità di Joomla
- il download di Joomla e i requisiti tecnici per l'installazione.

Joomla e l'interfaccia di Back-end:

- accedere al Back-end di Joomla
- la gestione degli utenti
- le opzioni di configurazione
- la gestione dei menu e dei contenuti
- le varie estensioni di Joomla
- modalità di installazione e disinstallazione delle estensioni.

La configurazione:

- configurazione globale del sito
- configurazione di sistema
- configurazione del web server.

Gestire gli accessi:

- aggiungere un nuovo utente
- conferma attivazione account
- modifica profilo utente
- settare i permessi
- tipologie di utenti: configurazione standard e personalizzazione.

Curare l'accesso ai contenuti:

- gestione dei contenuti e impostazione dei permessi
- tipologie dei permessi: impostazione e personalizzazione
- assegnare i permessi ai menu.

Gestione dei contenuti:

- gestione delle categorie
- livelli di accesso alle categorie create
- cenni sulla Gestione articoli
- creare un nuovo articolo
- la pubblicazione e la sospensione di un articolo
- personalizzare i livelli di permesso su un articolo aggiunto
- archiviare gli articoli e possibilità di ripristinarli
- editor visuale per la gestione dell'Editing dei contenuti
- la gestione dei parametri per il modulo Articoli.

Obiettivi

Il partecipante acquisisce una buona conoscenza di base del CMS Joomla e sarà in grado di installare, personalizzare e gestire siti con Joomla.

Destinatari

Quanti vogliano realizzare e gestire siti internet e portali utilizzando Joomla.

Prerequisiti

Conoscenze di base di informatica.

Pubblicazione di contenuti su Web con piattaforme open source

Imprese, Pubblica Amministrazione e mondo della ricerca guardano, per l'offerta di servizi e contenuti sul Web, con crescente interesse al mondo open source. Ciò è dovuto soprattutto alla ricchezza dei prodotti sviluppati da una comunità sempre più vasta e professionale, che ha permesso di migliorare la qualità, le prestazioni e la facilità di amministrazione.
In quest'ambiente sta avendo diffusione la combinazione di Apache come server Web, MySQL come database e PHP come linguaggio per la gestione di contenuti dinamici, acquisibili da distribuzioni multipiattaforma come XAMPP.
Il corso ha carattere molto pratico e applicativo, con sessioni di esercitazione che, a partire dalla seconda giornata, consentiranno al partecipante di sviluppare un proprio sito con applicazioni diverse.
Saranno messi a confronto i CMS (Content Management System) più diffusi al fine di poter individuare il più adatto al sito che si vuole progettare.

Agenda (3 giorni)

Configurazione di sistema:

- installazione del server Apache
- installazione di PHP
- installazione di MySQL
- installazione di phpMyAdmin (mysql web administration tool).

Creazione di contenuti dinamici:

- integrazione di PHP ed HTML
- accesso a DataBase con PHP.

Configurazione di un Content Management System:

- struttura di un CMS e criteri di selezione
- installazione e configurazione di Joomla
- installazione e configurazione di WordPress
- installazione e configurazione di Drupal
- amministrazione (moduli, blocchi, temi, menu e reportistica)
- contenuti
- gestione utenti
- tassonomia (taxonomy)
- prestazioni (performances)
- triggers e actions
- views.

Obiettivi

Al termine del corso i partecipanti saranno in grado di operare in un ambiente open source e di poter individuare la piattaforma più adatta alle proprie esigenze.

Destinatari

Responsabili siti WEB e portali. Responsabili IT.

Prerequisiti

Amministrazione di un server Unix e linguaggio html di base.

Progettazione Object Oriented con UML

Il corso illustra le tecniche fondamentali per la progettazione object-oriented di sistemi software utilizzando il linguaggio UML 2 per la documentazione degli artefatti prodotti. I principali argomenti trattati sono le architetture del software, il modello di progettazione e gli aspetti più importanti della progettazione di dettaglio.

Agenda (3 giorni)

Concetti generali:

- elementi fondamentali di un processo di sviluppo del software
- caratteristiche del modello di sviluppo iterativo e incrementale
- relazione fra l'analisi e la progettazione object-oriented
- introduzione al linguaggio di modellazione UML 2
- concetti fondamentali del modello object-oriented: classi e istanze, messaggi, operazioni, metodi, information hiding, ereditarietà
- architetture del software
- architetture e stili architetturali
- tipologie di architetture: architettura multi-tier, architettura basata su componenti, architettura orientata ai servizi.

Il modello di progettazione:

- partizionamento del sistema software in sottosistemi
- individuazione e caratteristiche dei sottosistemi
- progettazione dei componenti: ruoli e modelli dei componenti, interfacce
- scelta del middleware per la comunicazione remota.

La progettazione di dettaglio:

- trasformazione e raffinamento del modello di analisi nel modello di progettazione
- progettazione degli oggetti (oggetti transienti e persistenti, oggetti attivi e passivi)
- determinazione della visibilità degli attributi e delle operazioni
- attributi di classe e d'istanza
- attributi derivati
- i costruttori degli oggetti
- le relazioni fra le classi: generalizzazione, associazione, aggregazione, dipendenza, realizzazione
- analisi e trasformazione delle relazioni fra le classi: relazioni derivate;
- la delegazione come alternativa all'ereditarietà
- progettazione delle relazioni fra le classi
- tecniche di modularizzazione
- principi di coesione e di accoppiamento fra moduli
- principi di progettazione object-oriented
- i principali design pattern: Model-View-Controller (MVC), Observer, Bridge, Abstract Factory, Singleton, ...

Transizione dalla progettazione alla programmazione object-oriented.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante avrà acquisito le tecniche per effettuare la progettazione object-oriented con UML e sarà in grado di usare i diagrammi UML per documentare gli artefatti di progettazione.

Destinatari

Analisti e Progettisti di applicazioni software; Responsabili di progetti software.

Prerequisiti

Conoscenza del linguaggio Java.



Progettazione e Governance di architetture SOA

Il corso illustra le metodologie e gli strumenti necessari per l'implementazione di una Service-Oriented Architecture (SOA) il cui obiettivo è avvicinare il business aziendale all'IT. Durante il corso sono illustrate le principali metodologie e le best practices in ambito SOA, analizzando la filosofia alla base della SOA stessa. Sono altresì esaminate le tecnologie e le piattaforme (Commerciali e Open Source) di mercato per traguardare efficientemente il risultato.

Agenda (3 giorni)

Introduzione alla System Integration.

Concetti fondamentali SOA.

Vantaggi e rischi di una SOA.

Impatti: organizzativi, strategici, economici e tecnologici.

SOA Components:

- infrastruttura ed esposizione dei servizi
- i Web Services
- Enterprise Service Bus (ESB)
- SOA Information e SOA Application
- introduzione al BPM e l'orchestrazione di servizi.

SOA Design:

- filosofia e metodologia in ottica SOA
- progettazione di un web service e di un business service
- patterns di progettazione e sviluppo
- registry e documentazione
- casi d'uso.

SOA Management:

- SOA Governance
- SOA Security
- Service level agreement
- SOA Roadmap.

SOA Platform:

- tecnologie e framework (commerciali ed open source)
- soluzioni proposte.

Obiettivi

Al termine del corso il partecipante acquisisce le basi sul paradigma SOA, sulle metodologie di progettazione, implementazione e governance e una piena visione delle differenti tecnologie utilizzate in ambiti SOA.

Destinatari

Architetti software, analisti, e programmatori di applicazioni di business. Responsabili di progetto e System Integrator.

Prerequisiti

Wsdl, xml, xsd (consigliate ma non indispensabili).



XML e SOA

Lo sviluppo di applicazioni Web in ottica Cloud impone la creazione di infrastrutture software basate su Architetture Orientate ai Servizi. Per comprenderne le potenzialità, è importante focalizzare l'attenzione sull'interoperabilità dei protocolli per l'implementazione dei servizi (XML e SOA).
Il corso illustra le metodologie e gli strumenti necessari per l'implementazione di una Service-Oriented Architecture (SOA) il cui obiettivo è avvicinare il business aziendale all'IT. Durante il corso sono illustrate le basi dell' XML come standard "de facto" per la rappresentazione dei dati, i principi di base dell'architettura SOA e le principali metodologie, analizzando la filosofia alla base della SOA stessa. Sono altresì esaminate le tecnologie e le piattaforme (Commerciali e Open Source) di mercato per traguardare efficientemente il risultato.

Agenda (3 giorni)

Introduzione alla System Integration.

Concetti fondamentali SOA.

Introduzione al linguaggio XML:

- concetti base di XML, uso e benefici
- Campi applicativi di XML
- XML e il mondo WEB.

La sintassi:

- definizione della grammatica: DTD
- l'evoluzione della grammatica: introduzione all'XML Schema.

La pubblicazione dei documenti XML:

- XSLT: il linguaggio per la presentazione
- gli scenari delle presentazioni: HTML,WML e SVG

XML dal lato della programmazione:

- il parser XML: come costruire l'albero del documento
- l'interfaccia del DOM: Document Object Model.

SOA Components:

- infrastruttura ed esposizione dei servizi
- i Web Services
- Enterprise Service Bus (ESB)
- SOA Information e SOA Application.

SOA Design:

- filosofia e metodologia in ottica SOA
- progettazione di un web service e di un business service
- casi d'uso.

SOA Platform:

- tecnologie e framework (commerciali ed open source).

Impatti: organizzativi, strategici, economici e tecnologici.

Obiettivi

Al termine del corso il partecipante acquisisce le basi sul paradigma SOA, sulle tecnologie abilitanti quali XML, una panoramica sulle metodologie di progettazione ed implementazione.

Prerequisiti

Conoscenza del funzionamento di una web application o di architetture multi livello.



Service-Oriented Architecture (SOA): orchestrazione e integrazione di servizi di business

Il corso presenta la Service-Oriented Architecture (SOA) e il nuovo approccio della service-orientation per l'implementazione dei servizi di business e la progettazione di applicazioni composite realizzate attraverso l'orchestrazione dei servizi di business. Gli aspetti tecnologici vengono realizzati nel contesto della piattaforma Java Enterprise Edition e vengono anche discussi gli aspetti di interoperabilità dei web services Java con I web services .NET.

Agenda (3 giorni)

I web services XML:

- introduzione alla piattaforma Java Enterprise Edition
- Web service XML e differenza con i web services HTML
- le tecnologie alla base dei web services XML: XML; WSDL; SOAP; UDDI
- caratteristiche delle interfacce WSDL
- il protocollo SOAP
- relazione fra i web services XML e i servizi di business e tecnici
- i web services nel contesto della SOA.

Sviluppo dei web services con JAX-WS:

- introduzione a JAX-WS: differenze fra JAX-WS 2.x e JAX-RPC 1.1
- sviluppo di web service sincroni e asincroni
- i tool wsimport e wsgen
- Deployment dei web services
- registrazione di un web service in un registro UDDI
- creazione dei web service e dei client e interoperabilità dei Enterprise Java Bean.

Realizzazione di applicazioni composite:

- orchestrazione e coreografia di web services
- il linguaggio BPEL
- realizzazione del workflow, deployment ed esecuzione di un'applicazione composita.

Introduzione alle tecnologie per i web services e ai principali servizi WS-*:

- WS-Security, WS-Addressing, WS-Reliable Messaging, WS-Policy
- ottimizzazione del trasporto dei messaggi SOAP
- SOAP with Attachments API for Java (SAAJ)
- interoperabilità fra i web services Java e i web services .NET.

Esercitazioni.

Obiettivi

Al termine del corso il partecipante acquisisce conoscenze di base sulla Service-Oriented Architecture (SOA) e sull'analisi e progettazione di servizi di business tramite l'utilizzo dei web services XML, nonché sugli aspetti di interoperabilità fra i web services Java e quelli .NET.

Destinatari

Architetti software, analisti, e programmatori di applicazioni di business. Responsabili di progetto e System Integrator.

Prerequisiti

Conoscenza del linguaggio Java e del linguaggio XML.



Evoluzione delle applicazioni per l'e-business dalle web application verso la Service-Oriented Architecture (SOA)

Il corso fornisce una panoramica sulle architetture e sulle tecnologie Java/Open Source per lo sviluppo di applicazioni per l'e-business che vogliono evolvere verso la Service-Oriented Architecture (SOA). Il corso approfondisce gli argomenti relativi alle architetture, alle applicazioni web, alle applicazioni di business e fa comprendere il nuovo sviluppo service-oriented e le caratteristiche peculiari della SOA. Infine illustra gli aspetti importanti per l'integrazione e l'interoperabilità fra sistemi eterogenei e le tecnologie dei web services XML.

Agenda (3 giorni)

Le architetture per l'e-business:

- cos'è l'e-business e caratteristiche dei sistemi per e-business
- i sistemi per e-business: come sono strutturati e come vorremmo che fossero
- le architetture dei sistemi per e-business.

Le web application:

- introduzione alla piattaforma Java Enterprise Edition (Java EE)
- caratteristiche e struttura delle web application: pagine statiche e dinamiche, web component, …
- tecnologie Java EE per la realizzazione di web application: Java servlet, JavaServer Pages, JavaServer Faces
- il pattern layers e le architetture multi-tier
- il ruolo del web application server, o web container
- tecniche e best practices per realizzare applicazioni con alta disponibilità, scalabilità e fault tolerance.
- il concetto di pattern, il pattern MVC e i principali pattern Java EE del presentation layer
- i principali framework per lo sviluppo di web application (JavaServer Faces, Spring, …)
- introduzione alla progettazione di Rich Internet Application con le tecniche Ajax.

Le business application:

- caratteristiche di un'applicazione di business
- architettura basata su componenti e modelli dei componenti
- il nuovo modello degli enterprise Java Bean 3.0
- il ruolo dell'application server
- integrazione fra le web application e le applicazioni di business
- i principali pattern Java EE del business e integration layer
- tecniche e best practices per lo sviluppo di applicazioni di business.

Architetture service-oriented:

- architetture applicative, architetture enterprise e architetture service-oriented
- la Service-Oriented Architecture (SOA): aspetti culturali e tecnologici
- il concetto di servizio: servizi di business e servizi tecnici.

I web services XML:

- cos'è un web service: differenza fra i web services HTML e i web services XML
- modelli di comunicazione dei web services
- scenari di utilizzo dei web services: urbanizzazione della rete e interoperabilità
- aspetti di sicurezza, di transazionalità e di interoperabilità per i web services XML
- framework e API per lo sviluppo dei web services XML (Axis, JAX-WS, …)
- tecniche e best practices per lo sviluppo dei web services XML
- introduzione alle tecnologie e agli standard di riferimento per i web service: XML, WSDL, SOAP, UDDI.

Esemplificazioni.

Obiettivi

Fornire conoscenze sulle architetture e sulle tecnologie Java/Open Source e sulle problematiche legate all'evoluzione verso la SOA e sulle caratteristiche e sull'utilizzo dei web services XML.

Destinatari

Architetti software, analisti, e programmatori di applicazioni di business. Responsabili di progetto e System Integrator.

Prerequisiti

Conoscenze di base sullo sviluppo del software.



Sviluppo di applicazioni con il framework Spring

Spring permette di semplificare le fasi di progettazione e realizzazione di applicazioni Java, fornendo strumenti efficaci per la maggior parte delle componenti delle usuali architetture.
Nella prima parte del corso è presentato il principio IoC (Inversion of Control) che rappresenta la struttura portante di tutto il frame work e viene introdotta la programmazione per aspetti AOP (Aspect Oriented Programming).
Nella seconda parte sono proposti, a diverso livello di dettaglio, i moduli che compongono l'architettura Spring.

Agenda (3 giorni)



Introduzione al framework Spring.

Inversion of control e Dependency Injection.

Spring Container e Spring Beans.

Aspect Oriented Programming in Spring: servizi, definizione di aspetti e custom advices.

Servizi del business layer. Transazionalità programmatica, dichiarativa o annotation based. Servizi cross-cutting.

Gestione della persistenza. Realizzazione del data access layer. Interazione con JDBC e con framework ORM.

Lo strato di presentazione: MVC e Web Flow. Interazione con web framework di uso comune.

Applicazioni Spring.

Il modello di scurezza per le Spring Applications.

Architetture per le applicazioni Spring.

Obiettivi

Al termine del corso, i partecipanti saranno in grado di progettare ed implementare applicazioni basate su Spring, e di utilizzare le funzionalità offerte dal frame work.

Destinatari

Analisti, e programmatori di applicazioni.

Prerequisiti

Esperienza sulla piattaforma JEE.

System Integration: scenari, tecnologie e metodologie

Il corso illustra le metodologie e gli strumenti necessari durante le attività di System Integration. In particolare sono trattate le tematiche dell'EAI (Enterprise Application Integration) il cui obiettivo è l'interoperatività e l'organizzazione dello scambio di informazioni tra applicazioni aziendali eterogenee. Durante il corso sono illustrate le principali metodologie e le best practices in ambito System Integration, è proposta una overview sulle problematiche che tipicamente si presentano in tali contesti e sono indicate le azioni correttive da apportare di volta in volta.
Infine sono analizzate le tecnologie e le piattaforme (Commerciali ed Open Source) di mercato per traguardare efficientemente il risultato di integrazione.

Agenda (2 giorni)

System Integration:

- introduzione
- obiettivi della System Integration
- evoluzioni della System Integration.

Architetture d'integrazione:

- Enterprise Application Integration (EAI)
- strumenti per l'integrazione
- dall'EAI alla SOA.

Progettazione architetture EAI:

- modelli di integrazione
- metodologie di integrazione
- azioni correttive e problematiche frequenti
- best practices e casi d'uso reali.

Tecnologie e piattaforme per l'implementazione:

- implementazione soluzioni EAI
- prodotti commerciali
- prodotti open source
- overview prodotti.

Obiettivi

Al termine del corso il partecipante acquisirà le basi teoriche sulla System Integration e sulle relative metodologie di progettazione ed implementazione; avrà altresì una visione delle differenti piattaforme utilizzate in ambiti di System Integration.

Destinatari

Responsabili e professional IT. System integrator.

Prerequisiti

Java, Xml, UML (consigliate ma non indispensabili).



NG-OSS (Next Generation Operational Support System)

I Service Providers per poter essere competitivi devono continuamente differenziare e innovare i propri servizi. Ciò richiede un continuo aggiornamento e riconversione sia del Software e Sistema Operativo (OSS) adottati per gestire le Reti di TLC, sia dei Sistemi di Supporto al Business (BSS) usati per gestire le procedure operative.
Il corso illustra gli aspetti legati al tema della gestione delle reti e dei servizi nell'Information & Communication Technology (ICT), con particolare riferimento alle reti di nuova generazione.
Sono presi in considerazione i lavori e gli standard realizzati dal TeleManagement Forum (TMF) e dall'ITU-T.

Agenda (2 giorni)

Introduzione al TMN (Telecommunication Network Management).

Struttura OSI nel TMN.

Cenni sul protocollo SNMP.

TM Forum finalità.

Cenni sulle reti di telecomunicazioni e loro evoluzione.

Architettura e Framework NG-OSS (Next Generation Operational System Support).

TNA (Technology Neutral Architecture).

Processi orizzontali e verticali.

Introduzione ad eTOM (Enhanced Telecom Operation Map).

Service Management - ITIL (Information Technology Infrastructure Library).

Obiettivi e modelli del SID (Shared Information Data).

Unified Modeling Language (UML).

Cenni sul linguaggio XML.

Tecnologie di riferimento dei Web Services (WSDL, SOAP,UDDI).

Introduzione alla Service Oriented Architecture (SOA).

Introduzione alla NGN OSS e NGN2 (Next Generation Network Operation System and Software).

Obiettivi

Fornire una serie di Framework, standard e linee guida necessari per gestire in maniera efficiente le reti di nuova generazione ed i sistemi informativi che le supportano.

Destinatari

Il corso è rivolto a tutti coloro che direttamente (come fornitori di servizi) o indirettamente (come fruitori di servizi) sono coinvolti nel mondo ICT.

Prerequisiti

Conoscenza di base del mondo dell'ICT.



Usabilità ed accessibilità dei Siti Web e lo standard W3C

Negli ultimi anni la diffusione di internet, delle tecnologie e degli strumenti di comunicazione, ha avuto un'evoluzione sempre maggiore e le informazioni che circolano su Internet sono ormai necessarie e richieste da tutti. Per rendere il servizio fruibile sono state identificate, a livello internazionale, una serie di regole da seguire per realizzare i siti web (Standard W3C) affinché questi siano disponibili anche per le persone diversamente abili nonché da postazioni non particolarmente aggiornate.
Il corso introduce le regole dello Standard W3C alle quali attenersi al fine di realizzare siti web che siano fruibili da tutti, ed illustra i requisiti specifici della Legge Stanca (Legge 9 gennaio 2004, n.4).

Agenda (2 giorni)

Definizione di Accessibilità.

Definizione di Usabilità.

Definizione di Ergonomia.

Lo Standard W3c:

- cos'è il W3C
- linee guida per i contenuti accessibili (WCAG)2.0
- conformità.

La Legge Stanca:

- a chi si rivolge
- terminologia della norma
- contenuti della legge
- linee guida per l'accessibilità
- linee guida per l'usabilità
- livelli di conformità.

Riferimenti.

Obiettivi

Conoscere le regole per progettare e realizzare siti web utilizzabili da chiunque, anche con strumenti/tecnologie di navigazione non recenti.

Destinatari

Progettisti, responsabili e sviluppatori di siti web.

Prerequisiti

Conoscenza dei concetti alla base del funzionamento del web.



Usabilità: progettazione dei servizi e delle applicazioni

II mondo dei servizi è sempre più il terreno di battaglia sul quale si giocano sfide decisive per il successo degli Operatori: oggi, infatti, il Cliente è divenuto più sensibile anche al "modo" in cui i servizi possono essere offerti. Con i dispositivi mobili di nuova generazione l'Usabilità ha, dunque, assunto un ruolo strategico nella progettazione dei servizi e delle applicazioni.

Agenda (3 giorni)

Usabilità: definizioni e generalità:

- vantaggi, diffidenze e problemi
- confronto tra ergonomia e usabilità dei sistemi informatici.

Usabilità delle interfacce Software:

- capire: la psicologia cognitiva e lo sforzo cognitivo, la memoria e I 2 golfi dell'Usabilità
- realizzare: obiettivi del progetto, garantire la visibilità, proporre inviti e vincoli d'uso, fornire un adeguato modello concettuale, semplificare i compiti, restituire feedback e gestire l'errore
- valutare e misurare: test di usabilità condotti con o senza il contributo degli utenti, basati su metodi di survey (questionari) o con l'ausilio di strumenti automatici.

Il colore e l'usabilità, la ruota dei colori, accostamenti cromatici schemi cromatici.

Esempi: saranno esaminati alcuni siti allo scopo di valutare il livello di usabilità e lo sforzo cognitivo.

Obiettivi

Illustrare i principi dell'usabilità delle applicazioni informatiche, le metodologie e le fasi dello sviluppo delle applicazioni usabili.
Esempi di valutazione dell'usabilità di siti web.

Destinatari

Responsabili siti WEB e portali. Responsabili IT. Analisti e sviluppatori di applicazioni.

Prerequisiti

Nessuno.



Le piattaforme applicative per dispositivi mobili

La crescente diffusione di smartphone, il miglioramento della copertura a larga banda per terminali mobili e l’incremento di potenza di elaborazione e compatibilità dei terminali, sta rendendo sempre più utilizzabili, su dispositivi mobili, contenuti ed applicazioni sviluppate per il Web.
D’altra parte, la disponibilità sui terminali di dispositivi come i ricevitori GPS permettono di sviluppare applicazioni specifiche per questa tipologia di utilizzatori in mobilità, ad esempio nel settore turistico.

Agenda (3 giorni)

Google Android:

- Android SDK.

Apple IOS:

- iPhone SDK.

Nokia Symbian:

- Programming Environment.

Windows Phone:

- Windows Phone Developer Tools.

Obiettivi

Il corso si propone di presentare le principali piattaforme per dispositivi mobili e le caratteristiche dei loro ambienti di sviluppo tramite la realizzazione di una semplice applicazione demo.

Destinatari

Analisti e sviluppatori di applicazioni.

Prerequisiti

Programmazione Java e C in ambiente Unix.



Objective C per iOS

La crescente diffusione di dispositivi mobili Apple, (iPhone, iPad e iPod Touch) ha rivoluzionato il concetto di portabilità e ha reso utilizzabili contenuti ed applicazioni sviluppate per il Web.
Il corso illustra le caratteristiche del sistema operativo iOS focalizzandosi sugli aspetti legati alla progettazione delle applicazioni.

Agenda (4 giorni)



Introduzione al modello di programmazione Apple: XCode e Interface builder.

Fondamenti di programmazione con Objective-C.

Introduzione alle collections: NSArray, NSSet, NSDictionary.

Il modello Apple MVC.

Custom Views e View Controllers.

Event Handling con Objective-C.

Table e Table View.

MultiViews, Tab Bars, Pickers.

Autorotation, Autosizing.

Collegamento HTTP, XML parsing, Web navigation.

Introduzione alle mappe.

Obiettivi

Fornire le conoscenze sul sistema operativo iOS e gli strumenti per sviluppare applicazioni.

Destinatari

Analisti e sviluppatori di applicazioni.

Prerequisiti

Nessuno.

Android: progettazione di applicazioni per terminali mobili

Le prestazioni dei terminali mobili di ultima generazione sono determinate dal notevole sviluppo dei sistemi operativi utilizzati. Android è il sistema operativo open source – basato su Java - che si sta diffondendo con maggiore velocità, con grandi prospettive di sviluppo sia negli Smartphone, sia nei Tablet PC.
Nella parte iniziale del corso sono descritte le caratteristiche delle applicazioni per dispositivi mobili e l'architettura di Android. Si passa quindi alla progettazione delle applicazioni, con riferimento alla gestione dell'interfaccia grafica, ai servizi di localizzazione, comunicazione e networking, ai processi in background, alla distribuzione delle applicazioni.

Agenda (5 giorni)



Introduzione ad Android.

Descrizione di un'applicazione Android:
- installazione passo-passo dell'ambiente di sviluppo in Eclipse e del relativo plug-in ADT.
- creazione della prima applicazione.

Componenti e risorse:
- l'approccio dichiarativo di Android nella gestione delle risorse (CPU, memoria). Gli oggetti
- Drawable responsabili dell'aspetto grafico delle applicazioni.

Sviluppo di applicazioni per terminali mobili.

Activity e Intent.

L'interfaccia grafica:
- studio delle componenti grafiche di android.
- View e Layout
- Widget ed eventi
- Animation, Menù, Dialog e Toast.

Gestione dei dati:
- la gestione dei File e del DBMS SQLite.

Multithreading e servizi:
- la gestione dei Thread nell'ottimizzazione delle risorse. Realizzazione di attività in background.
- tecniche di sincronizzazione.

Utilizzo della rete e sicurezza.

Le Google Maps API:
- studio di due specializzazioni della classe View. Il Web Engine.
- visualizzazione e customizzazione delle Google Maps.

La gestione dei media.

Approfondimenti:
- il processo di pubblicazione
- test e Instrumentation
- sistemi di autenticazione
- gestione dei contatti.

Obiettivi

Fornire le conoscenze di base sul sistema operativo Android e su come sviluppare applicazioni in Java compatibili.
Comprendere le differenze rispetto ad altri modelli di programmazione.

Destinatari

Analisti e sviluppatori di applicazioni.

Prerequisiti

Nessuno.

Security Manager:
Sicurezza e protezione delle informazioni Personali e Istituzionali

Le organizzazioni e gli enti Istituzionali sia in ambito Internazionale che Europeo, in materia di "Security", si avvalgono, per tradizione, di strutture organizzative di indirizzo, di controllo e di gestione dell'operatività varie e molteplici, in funzione dei differenti aspetti di sicurezza: intelligence, safety, sicurezza fisica, sicurezza delle informazioni e delle reti di telecomunicazione, sicurezza informatica. Tuttavia l'evoluzione delle tecnologie e la globalizzazione delle comunicazioni e dei processi sociali, politici ed economici sta creando sovrapposizione e comunanza di ruoli, processi, metodi e strumenti per garantire protezione a vari livelli. Le competenze professionali, infine, sebbene siano spesso provenienti da ambiti accreditati a livello istituzionale, ad oggi necessitano comunque di alta qualifica manageriale, etica e leadership riconosciute, unitamente a competenze particolarmente avanzate e diversificate al fine di esercitare e concepire con sempre maggiore efficacia un ruolo che si sta andando sempre più ad innovare nella forma e nei contenuti a fronte del notevole incremento di nuove forme di attacco a un sistema interconnesso da tecnologie evolute (CyberSecurity).

Agenda (2 giorni)

Quadro di riferimento:

- codice "Privacy" (D.Lgs.196/03) e il prossimo "Regolamento Europeo in materia di protezione dei dati"
- aspetti organizzativi, responsabilità e ruoli di controllo e di gestione
- mappa delle competenze, skill, iter ottimale per avviare programmi di certificazioni professionali di processo
- misure di sicurezza logiche, fisiche ed organizzative a tutela del cittadino e delle Istituzioni
- modalità di supporto alla Autorità Giudiziaria.

Ambiti e Perimetri interessati

- Amministrazioni Pubbliche Centrali e Locali
- Enti a partecipazione statale
- analisi dei principali Standard "de Jure" e "de facto" in materia di sicurezza a protezione dal Cyber Crime
- processi, politiche e procedure operative da considerare
- casi di studio ed esempi
- cenni sulle tecniche di protezione tradizionali e sulle tecnologie emergenti (CyberSecurity).

Obiettivi

Acquisire una visione ad ampio spettro in materia di riservatezza delle informazioni e delle attuali misure di sicurezza logiche, fisiche e organizzative da adottare per la conformità e la corretta conservazione dei dati

Individuare le competenze, le responsabilità e le indispensabili suddivisioni di ruoli.

Destinatari

Responsabili IT, CIO (Chief Information Officer), CTO (Chief Technology Officer), Security Manager, CSO (Chief Security Officer), Titolari, Responsabili di trattamento dati, operatori nel settore della Security e della Gestione della Sicurezza, manager del settore di Security Intelligence, appartenenti alle Forze dell'Ordine e quanti operano nella gestione dei dati informatici e telematici particolarmente delicati.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

Data Privacy e Data Protection nelle Infrastrutture Critiche nazionali

Il trattamento, la riservatezza e la protezione dei dati personali, sensibili, particolari o comunque "critici" per le infrastrutture nazionali presenta rischi elevati e specifici. La normativa che tutela la privacy i diritti e le libertà fondamentali, le leggi in materia di sicurezza nazionale, antiterrorismo, antifrode, anticontraffazione si trovano sovente in parziale sovrapposizione. Se poi tali informazioni risiedono all'interno di asset e infrastrutture nazionali ecco che queste ultime divengono obiettivi "sensibili" del cyber crime. La giurisprudenza italiana, le leggi promulgate e modificate in virtù di emergenze nazionali (cfr. terrorismo, crimini informatici, ecc.), il prossimo "Regolamento Europeo in materia di protezione dei dati", individuano misure da applicare a protezione di Cyber attacchi sempre più sofisticati e diversificati. Il fenomeno dei social network e la geolocalizzazione dei terminali impone nuove metriche e strumenti per proteggere ambienti e asset tangibili e virtuali.

Agenda (3 giorni)

Quadro di riferimento:

- infrastrutture critiche nazionali e loro interdipendenza
- normativa nazionale in materia di riservatezza e trattamento delle informazioni
- direttiva e regolamento europeo per la protezioni dei dati
- reati informatici : Terminologie e tipologie di attacchi
- CyberSecurity: scenari evolutivi, Minacce e Vulnerabilità
- rapporto tra terminali e reti
- differenze tra Architetture Informatiche
- ambiti – web 2.0, web 3.0
- Home Protection, Work Protection
- Social Media ed entertainment (web reputation, digital identity)
- payment (phone, Laptop, Smartphone, tablet)
- sicurezza delle applicazioni
- criteri di protezione e livello di controllo tecnologico utilizzato nei processi
- gestione del rischio , conformità e governo delle infrastrutture
- misure di sicurezza logiche, fisiche e organizzative.
-

Obiettivi

Individuare le Infrastrutture Critiche Nazionali e i Centri preposti al controllo (CERT, CSIRT, ecc.).
Acquisire le conoscenze di base della normativa in materia di riservatezza e protezione dei dati.
Analizzare gli scenari tecnologici evolutivi e le tipologie di attacchi.
Confrontare i principali criteri di protezione con il livello di rischio residuo accettato.

Destinatari

Chief Security Officer, Data Protection Officer, Consultant Privacy, Responsabili IT, Security Manager, Incaricati al trattamento, e quanti operano nella gestione dei dati informatici e telematici.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.



Security vs Privacy: misure per la protezione e conservazione delle informazioni e dei dati di traffico telefonico e telematico

Il trattamento dei dati di traffico telefonico e telematico presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato. Tali informazioni, infatti, hanno una natura particolarmente delicata e la loro utilizzazione impropria può avere importanti ripercussioni sulla sfera personale dei soggetti interessati. La giurisprudenza italiana in materia di privacy /D.lgs 196/03, il provvedimento del Garante del 17/01/2008, le successive modifiche e integrazioni, le leggi promulgate e modificate in virtù di emergenze nazionali (cfr. terrorismo, crimini informatici, ecc.) e correlate (cfr. D.lgs 231/01) per adempimenti alla Convenzione di Bruxelles, individuano un insieme di accorgimenti e misure da porre in essere a garanzia degli interessati.

Agenda (3 giorni)

Quadro di riferimento:

- normativa in materia di protezione dei dati personali (D.Lgs.196/03 e correlate)
- provvedimenti e pronunciamenti del Garante in materia di Videosorveglianza
- misure minime di sicurezza previste dal Codice in materia di protezione dei dati personali
- misure di sicurezza da adottare dai provider di servizi di telecomunicazione di prestazioni a supporto della Autorità Giudiziaria incluse le intercettazioni.

Ambiti e Perimetri interessati ai trattamenti:

- Operatori e fornitori coinvolti
- informazioni e dati di traffico che devono essere conservati
- registrazione dei trattamenti, conservazione e cancellazione dei dati
- descrizione della documentazione necessaria e di come condurre verifiche periodiche.

Conformità, Misure di sicurezza e tecniche emergenti idonee per la protezione:

- misure di sicurezza logiche, fisiche e organizzative
- utilizzo di tecniche di protezione tradizionali (cfr. cifratura, firma digitale, DRM, DLP, ecc.)
- impatto delle tecnologie emergenti (CyberSecurity) e delle minacce correlate (CyberCrime).

Obiettivi

Acquisire un metodo strutturato, completo e pratico per condurre un progetto di assessment e compliance in materia di riservatezza delle informazioni.
Acquisire le conoscenze in merito alle misure di sicurezza da adottare per la conformità e la corretta conservazione delle informazioni e dei dati di traffico telefonico e telematico.
Individuare tra i requisiti richiesti dalla legge le tecniche idonee e più efficaci per la protezione dei dati.

Destinatari

Responsabili IT, Security Manager, Incaricati al trattamento, e quanti operano nella gestione dei dati informatici e telematici soggetti alla privacy.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

La regolamentazione dei servizi di TLC

La liberalizzazione del mercato dei servizi e delle reti di telecomunicazione ha rappresentato una discontinuità forte, sia nel mercato, che nell'evoluzione tecnologica di tutto il mondo ICT.
Sia per gli ex-operatori monopolisti che per i nuovi entranti nel settore, un ruolo centrale è giocato dagli accordi di interconnessione, che hanno un impatto decisivo sullo sviluppo dei servizi, sulle condizioni di competizione, sulla forma e sulla dimensione della concorrenza. Tenere conto delle varie implicazioni dell'interconnessione richiede una preparazione specifica che attinge a diversi ambiti disciplinari: tecnici, giuridici ed economico-contabili. Il corso fornisce un quadro dei principali problemi legati alla regolamentazione dell'interconnessione e dell'intero mercato ICT: presupposti tecnico-economici, scelte normative del legislatore europeo e di quello nazionale e prospettive di evoluzione nel futuro, con particolare riferimento al contesto italiano ed alla evoluzione della rete di accesso in ottica NGN2.
Per tutte le problematiche affrontate, è fatto un confronto fra la realtà italiana e le esperienze più significative del contesto internazionale.

Agenda (1 giorno)

La liberalizzazione dei mercati di TLC:

- le origini e i principi ispiratori
- i principi enunciati nel DPR 318/97 e nel DM 23 aprile 1998
- il ruolo dell'Authority
- OLO e ISP.**Interconnessione tra reti di operatori.**

La regolamentazione dei servizi di fonia:

- CS (Carrier Selection) e CPS (Carrier Preselection)
- servizio di raccolta
- servizio di terminazione
- servizio di transito.

Unbundling del Local Loop:

- modalità di ULL (ULL, Shared Access, Sub-loop).

Servizi a larga banda:

- Bitstream Access
- Backhaul.

Servizi di trasporto dedicato.

La regolamentazione nel VoIP:

- operatori ECS e PATS
- numerazione
- servizi avanzati.

Operatori virtuali.

Analisi dei mercati 1-14 della normativa italiana.

Evoluzione delle normative in vista delle reti NGN.

Obiettivi

Fornire una visione tecnico-economica degli aspetti normativi che regolano i vari settori del mercato delle telecomunicazioni, con particolare riferimento al contesto italiano.

Destinatari

Manager e Professional ICT.

Prerequisiti

Nessuno.

Gli aspetti giuridici nella regolamentazione del mercato di TLC

La libertà di informazione – intesa sia in senso attivo (come libertà di informare), sia in senso passivo (come libertà di essere informati), sia infine in senso riflessivo (come libertà di informarsi) – può essere considerata la pietra angolare degli ordinamenti democratici.
Ciò si è tradotto, per quanto riguarda l'ordinamento giuridico italiano, in una crescente attenzione del legislatore per la regolazione del mercato delle telecomunicazioni. Negli ultimi decenni si è passati infatti dal monopolio pubblico al servizio universale, attraverso due distinte stagioni di liberalizzazione. L'implementazione delle nuove tecnologie ha inoltre indotto l'ordinamento comunitario ad emanare un pacchetto di direttive sulle comunicazioni elettroniche, cui in Italia si è dato attuazione con il Codice delle comunicazioni elettroniche.
Si è quindi andato via via componendo un settore, quello delle TLC, variegato e complesso. Ciò si è riflettuto anche sulle relative attività di regolazione e di gestione, in riferimento alle quali le esigenze di governo vanno composte con quelle di garanzia. Tali compiti sono in parte svolti da organi con legittimazione democratica diretta o indiretta (Parlamento e Governo) e, per altra parte, da organi neutri e/o di garanzia, la cui legittimazione formalmente non è di natura democratica, ma tecnocratica, basandosi non tanto sulla investitura popolare diretta o indiretta, bensì sulla competenza tecnica: si tratta, nella specie, dell'AGCOM, dell'Autorità Antitrust e dei Co.re.com, con competenze differenziate a livello orizzontale e verticale, ma talvolta tendenti a sovrapporsi.

Agenda (1 giorno)

Telecomunicazioni e Costituzione.

Evoluzione della conformazione del mercato delle TLC: dal monopolio pubblico al servizio universale:

- la prima stagione di liberalizzazione
- la seconda stagione di liberalizzazione
- il servizio universale.

Le direttive comunitarie sulla comunicazione elettronica ed il codice delle comunicazioni elettroniche.

Funzioni di governo e di garanzia nella regolazione e nella gestione del settore delle TLC.

Le istituzioni democratiche:

- ruolo del Parlamento
- ruolo del Governo.

Le istituzioni tecnocratiche:

- l'autorità per le garanzie nelle comunicazioni (AGCOM): genesi, struttura e funzioni
- il riparto di competenze fra AGCOM ed Autorità Antitrust
- i Comitati regionali per le comunicazioni (Co.re.com): genesi, struttura e funzioni.

Obiettivi

Fornire un tool kit di conoscenze giuridiche sulla regolazione e sulla gestione del settore delle TLC, sia attraverso l'analisi dei principali provvedimenti normativi, sia con il monitoraggio della giurisprudenza più recente in materia. Il fine è quello di fornire strumenti utili ad apprendere quali siano le regole di comportamento e le tecniche di tutela, in via stragiudiziale e giudiziale, che gli operatori del settore devono seguire e possono utilizzare.

Destinatari

Manager e Professional ICT.

Prerequisiti

Nessuno.

Le Telecomunicazioni "senza formule"

Il corso illustra con linguaggio semplice e comprensibile a tutti, gli aspetti tecnici fondamentali che riguardano le moderne reti di telecomunicazione, descrivendone la tecnologia, le prestazioni e i contesti applicativi.
Si tratta di una panoramica sul mondo delle telecomunicazioni con argomenti che comprendono la telefonia fissa e mobile, le reti dati, le reti locali di computer (LAN) e il protocollo TCP/IP. Si parla anche di Internet e delle varie tecniche di accesso fisse e mobili (WiFi, ADSL, UMTS, ecc.).

Agenda (5 giorni)

Le basi delle telecomunicazioni:

- generalità e tipi di informazione
- tecnica analogica e tecnica digitale
- i mezzi trasmissivi: doppino, coassiale e fibra ottica
- la multiplazione
- la protezione contro gli errori
- la tecnica radio: frequenze, trasmettitori, ricevitori, antenne, propagazione.

Introduzione alle reti:

- generalità su reti e servizi
- reti a commutazione di circuito e di pacchetto
- architetture, prestazioni e servizi.

La rete telefonica fissa.

Le reti per dati:

- i protocolli e il modello OSI
- confronto tra le tecnologie, prestazioni e servizi.

Le reti locali di calcolatori (LAN).

La rete Internet:

- generalità e concetto di internetworking
- l'architettura di comunicazione TCP/IP
- indirizzi Internet, struttura e numerazione di una rete IP
- lo strato di trasporto: TCP e UDP
- cenni sul routing IP
- gli applicativi principali: Telnet, FTP, posta elettronica, ecc
- il Protocollo HTTP e il World Wide Web
- cenni sul linguaggio HTML
- accesso alla rete tramite ADSL, WiFi, WIMAX.

Le reti mobili:

- architettura cellulare
- il sistema GSM e le sue evoluzioni (GPRS e UMTS)
- servizi di base e a valore aggiunto
- trasmissione dati su reti mobili e accesso a internet da rete mobile.

Obiettivi

Il corso intende offrire, con un linguaggio comprensibile ad un uditorio di non tecnici, una visione d'insieme delle reti di TLC - fisse e mobili - di Internet e dei relativi servizi.

Destinatari

Figure professionali non tecniche.

Prerequisiti

Nessuno.

Reti di telecomunicazione: servizi, architetture e protocolli

Le reti di telecomunicazione sono state protagoniste nell'ultimo decennio di una rivoluzione che ne ha cambiato radicalmente i connotati tecnici e di servizio. Sono diventate, grazie all'avvento di Internet e dei servizi radiomobili, la vera e propria spina dorsale della società. Il corso illustra, con un approccio tecnico, i servizi, gli elementi costitutivi, le architetture e gli standard principali su cui si basano le moderne reti di telecomunicazione. Sono trattati in particolare gli standard come Ethernet e l'architettura TCP/IP, che hanno soppiantato standard più recenti (es. ATM, Frame Relay) e costituiscono la base per le attuali reti integrate multiservizio. L'obiettivo del corso è fornire una visione introduttiva, ma completa, sul mondo delle reti di telecomunicazione, dalle tecnologie ai servizi, a coloro che andranno ad operare nel contesto dell'ICT.

Agenda (5 giorni)

Introduzione alle reti di TLC:

- i servizi di TLC: dalla fonia al multimedia
- il trasporto delle informazioni; trasmissione analogica e digitale
- elementi costitutivi di una rete di TLC
- la qualità di servizio e la sicurezza nelle reti di TLC
- il modello ISO/OSI.

Le reti per fonia:

- la rete telefonica tradizionale
- le reti radiomobili
- i servizi evoluti e la rete intelligente.

Le reti per dati:

- la commutazione di pacchetto
- confronto fra le reti telefoniche tradizionali e le reti per trasmissione dati.

Le tecnologie legacy di Livello 2:

- ATM e Frame Relay.

La soluzione Ethernet (back to the future !):

- lo standard Ethernet
- gli switch e le reti Switched LAN
- Wireless LAN
- utilizzo di Ethernet in ambito metropolitano: reti Metro Ethernet.

Internet: architettura e servizi:

- generalità sull'architettura TCP/IP
- funzionamento di Internet: i router e il routing IP
- le applicazioni (e-mail, browsing, multimedia).

Tecnologie di rete per servizi multimediali:

- backbone multiservizio
- accesso a larga banda: le tecnologie xDSL
- evoluzione delle tecnologie per la mobilità
- le reti di nuova generazione (NGN).

Obiettivi

Descrivere, con un buon livello di approfondimento, i servizi, le architetture, i protocolli e gli standard su cui si basano le moderne reti di TLC.

Destinatari

Personale di operatori di TLC e di Service Providers.

Prerequisiti

Nessuno.

I cablaggi strutturati negli edifici e nei Data Center: progettazione e normative

La progettazione dei cablaggi strutturati assume importanza sempre maggiore negli edifici moderni.
Un sistema di cablaggio strutturato supporta oltre la fonia e lo scambio di dati, anche il controllo accessi, dell'energia e delle condizioni climatiche, la diffusione audio e video, la sicurezza.
Il corso tratta le normative CEI-EN 50173 e CEI-EN 50174, e ne descrive l'applicazione pratica basandosi, se possibile, anche su casi reali proposti dai partecipanti. A questo scopo, essi dovranno dotarsi, per poter impostare e definire il progetto del loro caso di studio, di tutte le informazioni utili e delle planimetrie degli edifici o Data Center (preferibilmente su carta), necessarie per svolgere il lavoro individuale.

Agenda (3 giorni)

Richiami sui mezzi trasmissivi:

- cavi e i componenti di cat. 5, 5E, 6, 6A, 7
- le fibre ottiche multimodali OM2, OM3 e OM4
- le fibre ottiche monomodali OS1 e OS2.

Progettazione del cablaggio strutturato di un edificio o comprensorio secondo le normative Italiane ed Europee:

- CEI-EN 50173 parte 1ª, 2ª, 3ª
- CEI-EN 50174 parte 1ª e 2ª
- le equazioni di canale per il calcolo del Channel
- messa a terra, equipotenzialità e la normativa Europea EN 50310.

Trattazione della guida CEI 306-10 riguardante la realizzazione di un cablaggio strutturato e l'applicazione delle norme tecniche.

Criteri di progetto di un cablaggio strutturato:

- dimensionamento delle dorsali
- calcolo dell'attenuazione di tratta in fibra e conformità ai limiti degli standard di rete
- dimensionamento del cablaggio di piano.

Progettazione del cablaggio nei Data Center:

- le specifiche della normativa Europea CEI-EN 50173 parte 5ª
- i differenti approcci "Top of Rack" e "End of Row"
- le distanze massime ammesse per le connessioni Fiber Channel 2, 4, 8, 10 Gb/s.

Il collaudo finale dei cablaggi secondo le varie categorie.

Casi di studio reali dei partecipanti:

- presentazione dei casi di studio
- applicazione degli standard e dei criteri di progetto ai casi reali.

La documentazione di progetto e di fine lavori:

- tracciati canaline su planimetrie
- dimensionamento dei rack e posizionamento dei componenti passivi e attivi.

Obiettivi

Fornire le conoscenze e i criteri di progetto di una rete di edificio o di Data Center, basandosi sulle normative Italiane (CEI) ed Europee (EN).

Destinatari

Sistemisti e tecnici di rete.

Prerequisiti

Conoscenza di base delle LAN e di elettrotecnica.



Evoluzione delle reti per fonia

Le reti telefoniche hanno avuto negli anni una continua evoluzione tecnologica, a partire dalla digitalizzazione della trasmissione, fino ad arrivare alle tecnologie di Voice over IP, che ne stanno radicalmente cambiando i connotati tecnologici e di servizio.
Il corso descrive l'architettura sia delle reti per telefonia funzionanti in base al principio della "commutazione di circuito" sia di quelle, oggi sempre più emergenti, che adottano invece il principio della "commutazione di pacchetto", basate sul paradigma del mondo Internet, e cioè il VoIP. Vengono anche fatti cenni essenziali ad aspetti di dimensionamento, di qualità del servizio, e di costi/benefici delle diverse soluzioni tecnologiche.
Le presentazioni sui diversi argomenti si avvalgono di numerosi esempi con frequenti occasioni di discussione e interazione con i partecipanti.

Agenda (3 giorni)

Richiami alla rappresentazione di segnali audio (e video).

La codifica tradizionale PCM e i nuovi codec Audio: confronti prestazionali.

Problemi e soluzioni per la qualità dei segnali audio e video in reti a commutazione di circuito (TDM) ed in quelle a pacchetto (IP):

- rumore
- eco
- ritardo
- jitter.

La segnalazione a canale comune N. 7:

- I protocolli MTP, ISUP
- I protocolli per i servizi di "rete Intelligente" e per le reti cellulari.

Richiami al funzionamento delle reti IP.

Gestione dei servizi voce, e di servizi avanzati (video, instant messaging) tramite una rete a pacchetto IP.

La segnalazione per telefonia e servizi multimediali nelle reti IP.

Introduzione ai principali protocolli delle reti multimediali IP:

- SDP
- SIP
- Megaco (H.248)
- RTP.

Interlavoro fra reti tradizionali e reti IP.

Aspetti di sicurezza per i servizi multimediali su rete IP.

Dimensionamento delle reti di telecomunicazione ed analisi delle diverse alternative (circuito, pacchetto, reti ibride).

Obiettivi

Descrivere l'architettura delle reti per telefonia che si basano sulla "commutazione di pacchetto", e i protocolli di segnalazione per il trasporto della voce su IP.

Destinatari

Ingegneri di rete di operatori fissi e mobili, Tecnici di rete delle aziende manifatturiere di apparati per TLC.

Prerequisiti

Conoscenze di base delle reti di TLC.



Evoluzione dei Servizi e delle Reti di TLC

Il corso presenta le tendenze evolutive attuali e future del mercato dei servizi di TLC e delle tecnologie di rete per l'offerta di servizi multimediali e interattivi: dall'integrazione dei servizi tradizionali di TLC e dei media, fino ad arrivare al modello Triple Play, sia nel campo delle reti fisse che mobili, fino alla integrazione fisso-mobile e quindi al modello Quadruple Play.
La convergenza viene esaminata sul piano dei servizi e su quello delle reti; pertanto viene fornito un quadro, il più completo possibile, degli scenari di mercato, delle tecnologie abilitanti e delle architetture di rete per le offerte di servizi innovativi multimediali.

Agenda (2 giorni)

Evoluzione dei servizi di TLC.

Evoluzione delle reti verso la larga banda.

La convergenza dei servizi:

- convergenza TLC-Media (I-TV e Web-TV)
- convergenza fonia-dati: VoIP
- codifiche vocali
- trasporto della voce su reti IP: aspetti protocollari
- soluzioni tecnologiche
- servizi avanzati di telefonia su IP
- esempi di offerte commerciali
- il modello Triple Play.

Tecnologie di rete per la convergenza dei servizi:

- tecnologie di backbone: il modello "all IP"
- alternative tecnologiche ed architetturali per la rete d'accesso
- sistemi DSL
- reti in fibra ottica, reti ottiche passive
- Wireless Local Loop: Wi-Max e Wi-Fi; evoluzione delle tecnologie per la mobilità
- dal GSM all'UMTS ed evoluzione verso il 4G; la convergenza dei servizi mobili.

Convergenza fisso-mobile:

- integrazione commerciale e a livello di rete
- convergenza dei servizi
- dal Triple Play al Quadruple Play.

Il ruolo delle reti di nuova generazione (Next Generation Networks) nella convergenza delle reti e dei servizi.

Il ruolo della evoluzione dei dispositivi d'utente nella convergenza dei servizi.

Il ruolo degli operatori virtuali nella convergenza.

Obiettivi

Illustrare il processo di convergenza in atto, a partire dall'integrazione dei servizi tradizionali di TLC e dei media, fino alla integrazione fisso-mobile.

Destinatari

Personale tecnico e non tecnico di operatori di TLC e Service Providers.

Prerequisiti

Conoscenza di base di architetture e tecnologie tradizionali delle reti di TLC, per fonia e per dati e del protocollo IP.

NGN (Next Generation Networks): le reti di TLC di nuova generazione

L'evoluzione delle reti di telecomunicazioni a larga banda ha incentivato lo sviluppo di servizi multimediali e la convergenza con i servizi tradizionali. Originariamente sviluppate per la trasmissione dati e i servizi Internet, le reti Ethernet e IP oggi sono sempre più utilizzate per l'integrazione di servizi che ne sfruttano le potenzialità e la flessibilità quali la fonia e la televisione.
Di conseguenza si è sviluppato un modello di rete che, a partire dalla connettività IP, consente di fornire servizi avanzati in modo semplice ed efficiente. Tale paradigma, denominato NGN (Next Generation Network) prevede la separazione funzionale fra la parte trasmissiva della rete, la logica di controllo e quella di sviluppo delle applicazioni. Questa filosofia trova sempre maggiore applicazione nelle reti degli operatori di TLC, attraverso piattaforme di controllo centralizzate, piattaforme applicative aperte, tecnologie di backbone per l'integrazione di servizi multimediali e tecnologie per l'accesso con prestazioni sempre più elevate.

Agenda (2 giorni)

Introduzione:

- perché le reti di nuova generazione
- dalle piattaforme verticali alle "architetture orizzontali".

La convergenza dei servizi di telecomunicazioni.

Convergenza dei servizi di fonia e trasmissione dati:

- architetture di rete per VoIP.

Convergenza dei servizi televisivi e di telecomunicazioni:

- IP-TV.

Il modello 3Play.

Le attuali reti di telecomunicazioni:

- evoluzione della rete telefonica
- le reti per dati
- evoluzione dei servizi e delle reti mobili.

Convergenza fisso-mobile: il modello 4 Play.

Limiti nella implementazione della convergenza su reti di TLC tradizionali.

Architettura della rete NGN.

Il Backbone multi servizio: il modello "all IP" e la gestione della QoS.

Il piano di servizio della NGN: IMS (IP Multimedia Subsystem).

La rete d'accesso di nuova generazione.

Obiettivi

Il corso, oltre a fornire una panoramica sulle linee evolutive delle reti di TLC in ottica NGN, consente un approfondimento per ognuno dei mattoni fondamentali che costituiscono una rete di nuova generazione.

Destinatari

Ingegneri di rete di operatori fissi e mobili, Tecnici di rete delle aziende manifatturiere di apparati per TLC.

Prerequisiti

Conoscenze di base sulle reti di telecomunicazioni e sul protocollo IP.

Televisione digitale e standard DVB

La TV digitale, oggi largamente diffusa, sia con accesso fisso (satellitare e terrestre) che mobile, è abilitata tecnicamente grazie a due standard fondamentali: MPEG e DVB. MPEG (Moving Picture Experts Group) nasce come insieme di tecniche per la compressione dei contenuti audiovisivi digitali, ma oggi vanta diverse varianti che hanno la finalità di definire regole per la fornitura di servizi multimediali. DVB (Digital Video Broadcasting) indica lo standard europeo di trasmissione televisiva in tecnica digitale su varie piattaforme. Ha trovato la sua prima applicazione nella diffusione di programmi televisivi, attualmente è il protagonista del passaggio della diffusione televisiva terrestre alla tecnica digitale (TV digitale terrestre) ed è anche impiegato nella trasmissione televisiva via cavo e nella mobile TV ricevibile su dispositivi palmari (DVB-H). Il corso introduce l'insieme delle tecniche relative alla tv digitale, dalla digitalizzazione del segnale audiovisivo analogico, alle tecniche di compressione, in particolare lo standard MPEG. Descrive poi le caratteristiche e gli aspetti tecnici dello standard DVB, nelle sue varie declinazioni, e le ultime frontiere della TV ad alta definizione.

Agenda (3 giorni)

Introduzione al DVB-Project.

Richiami sui sistemi televisivi analogici.

Digitalizzazione del segnale televisivo analogico.

La compressione del segnale audiovisivo - MPEG:

- panoramica sugli standard MPEG-1 MPEG-2 e MPEG-4
- codifica MPEG 1-2 Video
- codifica MPEG-1 Audio. Estensione MPEG-2 Audio: suono multicanale. Compatibilità con MPEG-1
- codifica del video secondo MPEG-4 parte 10 (H.264)
- dati ausiliari: teletext, grafica, sottotitoli; inserimento pacchetti IP (DVB-H) e applicazioni per interattività (DVB-T)
- accesso condizionale
- formazione del Transport Stream
- evoluzioni dello standard MPEG.

La TV ad alta definizione (HDTV):

- generalità, definizioni, situazione attuale e problemi relativi alla standardizzazione
- tecniche di compressione, piattaforma satellitare e terrestre e occupazione di banda
- caratteristiche e struttura degli attuali televisori LCD e Plasma
- convivenza SDTV-HDTV, upscaling e downscaling, sorgente Blue Disc, interfacce digitali e analogiche.

DVB-T-H: Aspetti trasmissivi:

- pretrattamento del flusso dati
- modulazione OFDM e adattamento ai canali RF VHF e UHF
- struttura del segnale: supertrame, trame, simboli, celle
- segnali di controllo: continual pilots, scattered pilots, TPS
- calcolo del Net data rate per le varie combinazioni di parametri
- reti di diffusione: SFN, MFN e k-SFN
- copertura del territorio. Ripetitori e gap-filler
- problemi di sincronizzazione.

DVB-2.

La TV 3D.

Obiettivi

Illustrare le tecniche per la digitalizzazione del segnale video con riferimento allo standard DVB ed alle sue applicazioni.

Destinatari

Responsabili e tecnici interessati al digitale terrestre e alla mobile TV.

Prerequisiti

Conoscenze di base sulla codifica digitale dei segnali e dell'informazione.



Sistemi di trasmissione radio via satellite

Il corso offre una trattazione molto completa dei vari aspetti inerenti la trasmissione digitale via radio, applicata in particolare al caso del satellite. Sono trattati gli aspetti di modulazione, sincronizzazione e protezione dagli errori. Si trattano infine gli aspetti di qualità del collegamento, con la definizione delle misure di caratterizzazione in ambiente di laboratorio e in campo.

Agenda (5 giorni)



Tecniche di modulazione:

- il modello della trasmissione numerica
- spettri di potenza dei segnali modulati
- lo spazio dei segnali
- rivelazione coerente di segnali modulati in presenza di rumore
- rivelazione non coerente di segnali modulati
- efficienza energetica e spettrale delle modulazioni
- prestazioni delle modulazioni in presenza di canali Rayleigh lenti e non selettivi
- modulazioni Spread Spectrum e loro prestazioni
- modulazioni OFDM (Orthogonal Frequency Division Multiplexing) e loro prestazioni.

Sistemi e tecniche di sincronizzazione:

- stima della fase di un'onda non modulata
- stima della fase di onde modulate non a massima verosimiglianza
- stima della fase di un'onda modulata a massima verosimiglianza
- stima del tempo di simbolo a massima verosimiglianza, dati non noti
- stima del tempo di simbolo a massima verosimiglianza, dati noti
- stima del tempo di simbolo non a massima verosimiglianza

Tecniche di protezione dagli errori:

- generalità sulla teoria dell'informazione e sulla codifica di canale
- tipologie principali di codici
- caratteristiche generali dei codificatori FEC
- codici lineari a blocchi e loro prestazioni
- codici ciclici a blocchi e loro prestazioni
- codici convoluzionali e loro prestazioni
- turbo codici e loro prestazioni
- codici Low-Density Parity-Check (LDPC) e loro prestazioni
- cenni alle modulazione TRELLIS.

Qualità dei sistemi e dei servizi nelle reti di TLC: parametri e misure:

- qualità dei sistemi e dei servizi nelle reti di telecomunicazioni: parametri e misure
- qualità della rete e qualità dei servizi: definizioni di base
- qualità offerta e qualità percepita
- modelli di valutazione e relazioni di passaggio
- il parametro MOS ed altri parametri soggettivi
- parametri di qualità del processo di commutazione a circuito e a pacchetto
- parametri di qualità nei processi trasmissivi
- parametri alle interfacce analogiche
- parametri di qualità nei processi trasmissivi
- parametri alle interfacce numeriche.

Obiettivi

Conoscere il funzionamento di un sistema di trasmissione satellitare e saperne valutare i parametri di qualità.

Destinatari

Tecnici impegnati nella gestione di sistemi trasmissivi digitali via satellite.

Prerequisiti

Conoscenza di base dei sistemi di elaborazione dei segnali e di trasmissione delle informazioni.



Reti Satellitari: aspetti applicativi

I sistemi satellitari sono caratterizzati da coperture molto estese, elevati ritardi di propagazione. Il loro uso per telecomunicazioni è fondamentale nelle aree e nelle situazioni non coperte da reti terrestri (traffico marittimo e aeronautico), nelle zone in cui le infrastrutture terrestri sono scarse o difficilmente realizzabili (divario digitale), in caso di disastri, nel caso di servizi di diffusione o multicast.
La conoscenza delle caratteristiche tecniche dei sistemi satellitari è importante al fine di ottimizzare l'uso di tali risorse e comprendere come limitare e compensare gli effetti delle caratteristiche più sfavorevoli e quindi, in definitiva, come ottenere un servizio efficiente con il miglior rapporto costi/prestazioni.

Agenda (2 giorni)

Breve storia delle comunicazioni satellitari.

Principali caratteristiche delle costellazioni orbitali più usate (GEO, LEO, MEO, HEO):

- caratteristiche geometriche dei collegamenti.

Architetture di reti satellitari.

Regolamentazione (allocazioni dello spettro) e standardizzazione.

Sistemi di diffusione e standard DVB. Cenni sul DAB.

Sistemi VSAT e architetture di sistemi DVB/IP/RCS:

- tecnologie basate su standard DVB/IP e DVB RCS.

Qualità del servizio:

- problematiche, soluzioni e prestazioni di TCP/IP via satellite
- soluzioni a livello applicativo (HTTP, IPA, XFTP, SPDY)
- canali telefonici su flussi IP e GSM su portanti satellitari.

Sicurezza dei dati.

Applicazioni e servizi:

- servizi mobili e fissi
- servizi multimediali.

Analisi di mercato, principali modelli previsionali di costi di sviluppo e di penetrazione di mercato.

Messa in opera di servizi con reti satellitari mediante i principali sistemi già operativi o in via di realizzazione.

Obiettivi

Al termine del corso i partecipanti saranno in grado:

- di comprendere i principi di funzionamento dei sistemi di telecomunicazioni satellitari
- di individuare le soluzioni atte a mitigare gli effetti delle caratteristiche più sfavorevoli
- quali servizi di telecomunicazioni delle proprie reti possono utilizzare reti satellitari.

Destinatari

Utilizzatori finali come aziende private nazionali, istituzioni pubbliche, compagnie di navigazione, compagnie aeree, capitanerie di porto, associazioni di naviganti diportisti o di porti turistici, forze armate, aziende multinazionali con sedi delocalizzate, organizzazioni ONG presenti nei paesi in via di sviluppo.

Prerequisiti

Nozioni generiche su Internet e su servizi di telecomunicazioni.

Reti Satellitari: Tecnologie, architetture e servizi

I sistemi satellitari sono caratterizzati da coperture molto estese, elevati ritardi di propagazione. Il loro uso per telecomunicazioni è fondamentale nelle aree e nelle situazioni non coperte da reti terrestri (traffico marittimo e aeronautico), nelle zone in cui le infrastrutture terrestri sono scarse o difficilmente realizzabili (divario digitale), in caso di disastri, nel caso di servizi di diffusione o multicast.
La conoscenza delle caratteristiche tecniche dei sistemi satellitari è importante al fine di ottimizzare l'uso di tali risorse e comprendere come limitare e compensare gli effetti delle caratteristiche più sfavorevoli e quindi, in definitiva, come ottenere un servizio efficiente con il miglior rapporto costi/prestazioni.

Agenda (3 giorni)

Architetture di reti satellitari.

Principali caratteristiche delle costellazioni orbitali più usate (GEO, LEO, MEO, HEO):

- caratteristiche geometriche dei collegamenti.

Canale di propagazione:

- propagazione troposferica (modello ITU)
- cenni ai principali modelli di propagazione per canali mobili.

Cenni sulle problematiche di strato fisico:

- modulazione
- codifica
- interallacciamento
- copertura multifascio
- interferenza cocanale
- rigenerazione a bordo.

Dimensionamento.

Regolamentazione (allocazioni dello spettro) e standardizzazione.

Accesso multiplo:

- tecniche classiche di accesso multiplo (FDMA, TDMA, CDMA)
- tecniche di assegnazione su domanda e a prenotazione di pacchetto.

Procedure di controllo della chiamata.

Handover e istaurazione della chiamata, handover in sistemi integrati.

Carico utile di comunicazione: funzioni e schemi di principio.

Apparati di bordo.

Sistemi di diffusione e standard DVB. Cenni sul DAB.

Sistemi VSAT e architetture di sistemi DVB/IP/RCS:

- tecnologie basate su standard DVB/IP e DVB RCS.

Aspetti di rete:

- architetture e prestazioni di sistemi basati su IP, incapsulamento IP su DVB.

Qualità del servizio:

- problematiche, soluzioni e prestazioni di TCP/IP via satellite
- soluzioni a livello applicativo (HTTP, IPA, XFTP, SPDY)
- canali telefonici su flussi IP e GSM su portanti satellitari.

Sicurezza dei dati.

Applicazioni e servizi:

- servizi mobili e fissi
- servizi multimediali.

Il segmento terrestre ed i relativi apparati.

Analisi di mercato, principali modelli previsionali di costi di sviluppo e di penetrazione di mercato.

Messa in opera di servizi con reti satellitari mediante i principali sistemi già operativi o in via di realizzazione.

Cenni sulla componente satellitare dell'UMTS.

Obiettivi

Fornire i dettagli tecnici di funzionamento dei sistemi di telecomunicazioni satellitari evidenziando le principali problematiche e indicando le soluzioni atte a mitigare gli effetti delle caratteristiche più sfavorevoli.

Destinatari

Operatori di telecomunicazioni satellitari che intendono approfondire tecniche di ottimizzazione della trasmissione satellitari per i servizi multimediali

Operatori di reti terrestri che vogliano conoscere le caratteristiche tecniche dei sistemi satellitari.

Prerequisiti

Conoscenze dei principi fondamentali delle telecomunicazioni.

Ottimizzazione delle codifiche e compressione sui Carrier satellitari

Il corso fornisce competenze sulla digitalizzazione dei segnali audio e video e sulle tecniche di compressione. Si considera in particolare lo standard MPEG e il suo utilizzo nelle applicazioni satellitari. Vengono poi descritte le tecniche di codifica di canale e gli elementi fondamentali di un sistema di trasmissione digitale.

Agenda (5 giorni)



Digitalizzazione dei segnali audio-video:

- digitalizzazione dei segnali audio
- il segnale video composito.

La compressione dei segnali video ed audio: codifica di sorgente:

- generalità sulla codifica di sorgente
- la compressione dei segnali audio
- la compressione dei segnali video.

La multiplazione dei segnali video ed audio:

- generalità sulla multiplazione
- il caso MPEG.

La codifica di canale:

- capacità del canale continuo gaussiano
- il cut off rate dei canali con codifica
- codici lineari
- codici convoluzionali
- codici Trellis
- turbo codici
- codici Low Density Parity Ceck.

Fondamenti della trasmissione numerica:

- architettura di sistemi di trasmissione numerica in banda base
- architettura di sistemi di trasmissione numerica in banda traslata
- il rumore e le sue caratteristiche, cifra di rumore
- segnalazione numerica in banda base
- segnalazione numerica in banda traslata
- Il rapporto S/N e E_b/n_0 e la probabilità di errore per i vari sistemi di segnalazione.

Obiettivi

Al termine del corso i partecipanti hanno le conoscenze e le competenze per comprendere il funzionamento di un sistema di trasmissione satellitare e saperne valutare le prestazioni dal punto di vista delle tecniche di digitalizzazione e compressione utilizzate.

Destinatari

Tecnici impegnati nella gestione di sistemi trasmissivi digitali via satellite.

Prerequisiti

Conoscenza di base dei sistemi di elaborazione dei segnali e di trasmissione delle informazioni.

Fondamenti della trasmissione numerica: il segnale dall'origine al transito su una fibra ottica

Il corso affronta i concetti di base della trasmissione numerica. Per illustrare i vari processi, si seguono le vicende di un segnale (per esempio, il segnale telefonico) dalla sua origine, al transito su un collegamento in fibra ottica della dorsale di trasporto, fino a presentare la struttura di una moderna rete di TLC in fibra ottica.

Agenda (3 giorni)

Definizioni preliminari:
- segnali analogici e segnali numerici
- modelli di rete TLC
- rete PSTN e nuove tecnologie IP
- circuiti a 2 fili e circuiti a 4 fili.

Struttura e funzioni di una rete trasmissiva.

Multiplazione a divisione di tempo.

Conversione analogico-numerica della voce:
- codifica della forma d'onda: PCM, DPCM, ADPCM, modulazione Delta
- codifica di sorgente: LPC-LTP con RPE, CELP, AMR.

Multiplazione numerica:
- multiplazione sincrona ed asincrona
- il concetto di giustificazione.

Le gerarchie numeriche:
- PDH (Plesiochronous Digital Hierarchy)
- SDH (Synchronous Digital Hierarchy).

Sistemi di linea per il trasporto di flussi numerici:
- funzioni e strutture
- codifica di linea
- interferenza intersimbolica e diagramma ad occhio
- temporizzazione
- rigenerazione.

Sistemi per la trasmissione su fibra ottica:
- schema del collegamento
- sensitivity e budget di potenza del collegamento
- effetto della dispersione
- le più importanti architetture di rete
- schema a blocchi di un percorso trasmissivo.

Esempi di reti di TLC basate su fibra ottica.

Obiettivi

Tratteggiare i concetti fondamentali di trasmissione numerica, fino a descrivere il percorso coperto dal segnale su un collegamento in fibra ottica della dorsale di trasporto.

Destinatari

Ingegneri e tecnici che operano sulle reti e sui sistemi trasmissivi.

Prerequisiti

Non sono richieste competenze particolari.



Evoluzione delle reti di trasporto trasmissive: dalla SDH alla PTN

Il corso descrive l'evoluzione in atto nel livello trasmissivo delle reti di trasporto, con la transizione verso sistemi orientati al pacchetto, per renderle sempre più flessibili, scalabili ed efficienti. Sono richiamati in apertura la struttura e i componenti di un sistema trasmissivo basato su fibra ottica in tecnologia SONET/SDH. Si descrive quindi la costituzione di un sistema WDM, con riferimento alla capacità di trasporto e alla componentistica utilizzata, e il processo di evoluzione verso la Optical Transport Network (OTN). Si presentano infine le varie soluzioni possibili per realizzare una Packet Transport Network (PTN) e in dettaglio la soluzione basata sul protocollo MPLS-TP.

Agenda (3 giorni)

Rete di trasporto:

- la rete di TLC: funzioni e principali tecnologie
- elementi della rete di trasporto trasmissivo
- i sistemi di gestione, supervisione e provisioning.

Sistemi in fibra ottica:

- fibre ottiche: caratteristiche fisiche, parametri trasmissivi
- sorgenti e fotodiodi: tipologie e parametri significativi
- amplificatori ottici: l'amplificazione in fibra (EDFA, Raman) e a semiconduttore
- sistemi ottici singolo canale
- sistemi con rivelazione coerente.

Reti SDH:

- funzioni e caratteristiche di una rete SDH
- gerarchia di multiplazione
- efficienza di trasporto di traffico a pacchetto
- sincronizzazione di rete
- tipologia di apparati
- protezione di rete.

Sistemi ottici multicanale:

- struttura di un collegamento WDM
- griglia ITU-T, bande ottiche, numero di canali
- Optical Transport Network e standard G.709
- multiplatori e demultiplatori di lunghezza d'onda
- commutatori ottici: ROADM basati su WSS.

Packet Transport Network:

- fondamenti della tecnologia Ethernet, prestazioni e limiti
- Carrier Ethernet vs MPLS-TP
- MPLS-TP: il transport profile
- soluzioni Full Packet ed Enhanced (Ibride): esempi di sistemi commerciali.

Obiettivi

Presentare la struttura e i componenti di una rete di trasporto in fibra ottica.
Descrivere l'evoluzione verso OTN e le tecniche di trasporto a pacchetto.

Destinatari

Ingegneri e tecnici che operano sulle reti e sui sistemi trasmissivi. Ingegneri di rete di operatori di TLC.
Ingegneri e tecnici di rete di aziende manifatturiere.

Prerequisiti

Conoscenze di base nel campo delle comunicazioni ottiche.

Sistemi di alimentazione, di emergenza e fiscalità energetica

L'evoluzione della rete di telecomunicazioni e l'introduzione di nuovi servizi impongono che i sistemi di alimentazione siano caratterizzati da:

- notevole flessibilità, per adattarsi al graduale incremento delle apparecchiature, correlato agli sviluppi di rete
- consumi energetici contenuti, ridotte necessità di manutenzione e massimo sfruttamento delle condizioni ambientali
- elevata affidabilità, per contribuire a incrementare la disponibilità della rete.

Per soddisfare al meglio tutti i requisiti citati, ci si orienta sempre più verso apparati modulari di media e piccola taglia e su architetture di impianto decentrate.
Nel corso sono trattate anche gli aspetti legati alla fiscalità energetica.

Agenda (3 giorni)

Parte I Progettazione degli Impianti Elettrici

Introduzione alla progettazione elettrica.

Caratterizzazione elettrica delle utenze.

Sistemi di alimentazione e relativi componenti:

- il sistema di alimentazione normale
- il sistema di alimentazione privilegiata
- vincoli edili ed impiantistici.

Sicurezza elettrica.

Impianto di terra.

Architettura distributiva e componenti.

Rifasamento.

Impianti elettrici di segnale.

Documentazione di progetto.

Normativa vigente.

Parte II - Sistemi di alimentazione di emergenza

Standard ETSI e normativa vigente.

Sistemi di alimentazione senza soluzione di continuità:

- sistemi in C.A (UPS): (statici, rotanti)
- sistemi in C.C. (Stazioni di Energia in cc: raddrizzatori e pannelli collettori)
- accumulatori stazionari al Pb acido.

Sistemi di alimentazione di riserva:

- gruppo elettrogeno
- quadro di comando e controllo
- quadro di scambio da rete a GE e viceversa
- quadro di parallelo
- dispositivi ausiliari.

Collegamenti in C.C.:

- in corda
- in barra
- dimensionamento - cadute di tensione.

Criteri di dimensionamento e di progettazione:

- impianti senza soluzione di continuità in C.C. (SE in cc)
- impianti senza soluzione di continuità in C.A. (UPS)
- impianti di riserva (GE).

Esercizio dei sistemi di alimentazione:

- criteri di impostazione
- problematiche.

Parte III - Gestione del Sistema Energia e Fiscalità Energetica

La norma ISO 50001.

Politiche di saving:
- audit energetici
- interventi di saving
- il saving energetico in TI.

Autoproduzione (Sistemi alternativi di alimentazione):
- impianti fotovoltaici
- celle a combustibile
- impianti eolici
- cogenerazione – Trigenerazione.

Vettori energetici gravati da fiscalità:
- elettricità
- gas
- carburanti
- altri combustibili.

Struttura oneri fiscali:
- modalità di applicazione ed esenzioni
- elettricità
- gas
- carburanti
- altri combustibili

Obblighi fiscali:
- soggetti
- tipologie (consumo, autoconsumo, etc).

Modalità operative di adempimento degli oneri fiscali:
- oneri “parafiscali”
- struttura oneri parafiscali
- modalità di adempimento
- esenzioni.

Obiettivi

Al termine del corso, i partecipanti conosceranno problematiche, architetture e soluzioni relative ai sistemi di alimentazione e avranno un’ampia panoramica sulla gestione del Sistema energia e Fiscalità Energetica.

Destinatari

Energy Manager.

Prerequisiti

Nessuno.



Qualità dei sistemi e dei servizi nelle reti di telecomunicazioni: parametri e misure

Una buona qualità della rete è determinante ai fini della qualità dei servizi offerti all'utente finale, soprattutto nel caso di offerte multimediali.
Il corso presenta anzitutto i concetti che presiedono alla definizione ed alla valutazione della qualità intrinseca di una rete di telecomunicazioni e di quella trasferita ai servizi su di essa veicolati e fruiti dalla clientela. Sono quindi presentati i metodi di misura analitici per la qualità offerta ed empirici per la qualità percepita. A conclusione del corso è prevista una parte pratica con la realizzazione di misure di qualità.
L'impostazione del corso è flessibile, per consentire un adeguamento in funzione del livello di approfondimento richiesto e dello spazio che si voglia dedicare alle esercitazioni.

Agenda (3 giorni)



Brevi richiami sulle reti di telecomunicazione.

Qualità della rete e qualità dei servizi: definizioni di base.

Qualità offerta e qualità percepita.

Modelli di valutazione e relazioni di passaggio.

Il parametro MOS ed altri parametri soggettivi.

Parametri di qualità del processo di commutazione a circuito e a pacchetto.

Parametri di qualità nei processi trasmissivi.

Parametri alle interfacce analogiche:
- equivalente di trasmissione (loss) e distorsione di ampiezza
- ritardo di gruppo e distorsione di fase
- rumore: tipi e classificazioni
- distorsione totale
- adattamento d'impedenza e bilanciamento
- aliasing
- codifiche con riduzioni di ridondanza
- eco
- applicazioni al servizio VoIP.

Parametri di qualità nei processi trasmissivi.

Parametri alle interfacce numeriche:
- classificazione nella definizione di "errore"
- classificazione del parametro BER
- parametri "tempo-discreti" (SES, ES, DM)
- caratterizzazione del fenomeno "jitter".

Qualità dei collegamenti su coppie simmetriche in rame.

Qualità della trasmissione su fibra ottica.

Qualità nei terminali d'utente: aspetti di protezione e sicurezza.

Rassegna dei principali riferimenti normativi e Raccomandazioni ITU-T.

Esercitazione pratica: realizzazione di misure dei principali parametri presentati nel corso.

Obiettivi

Descrivere il concetto di qualità intrinseca di una rete e come questa viene trasferita ai servizi fruiti dalla clientela. Illustrare i metodi di misura analitici per la qualità offerta, ed empirici per la qualità percepita.

Destinatari

Ingegneri e tecnici che operano sulle reti e sui sistemi trasmissivi. Responsabili di sistemi trasmissivi.

Prerequisiti

Buona conoscenza delle reti di TLC per fonia e per dati.



Monitoraggio del traffico di Rete

Tradizionalmente l'analisi del traffico si divide in due grandi famiglie:

- l'analisi pacchetto-per-pacchetto, che è finalizzata alla risoluzione di problemi puntuali
- l'analisi per flusso, ovvero raggruppando assieme pacchetti omogenei, che permette invece di realizzare un monitoraggio permanente delle attività di rete.

Scopo di questo corso è di illustrare i concetti e le metriche di base nell'analisi di rete, e di analizzare i protocolli e le metodologie più comuni di monitoraggio del traffico. Sono analizzati gli strumenti di monitoraggio del traffico più diffusi, e alcuni problemi reali e proposte soluzioni concrete. Alle sessioni di teoria, saranno affiancate esercitazioni pratiche sui concetti trattati.

Agenda (3 giorni)



Introduzione al monitoraggio del traffico di rete.

Metodologie di misurazione di rete: RFC 1242, RFC 2285, RFC 2432, RFC 1944, RFC 2544.

Metriche di base: throughput, latenza, pacchetti persi, jitter, throughput, disponibilità.

Misurazioni per link o end-to-end, inline o offline, attivo o passivo.

Introduzione a SNMP.

Monitoraggio di rete utilizzando SNMP: MIB II, bridge MIB, RMON, Cisco NBAR.

Monitoraggio orientato ai flussi: NetFlow, IPFIX e sFlow.

Analisi degli accessi di rete e misurazione del traffico utilizzando RADIUS.

Alcuni casi reali di monitoraggio di rete.

Cattura dei pacchetti di rete: problematiche, tap vs port span, tipologie di reti.

Librarie per la cattura del traffico di rete: libpcap e PF_RING.

Analisi del traffico basato su pacchetti: concetti di base (TCP/IP), analisi di protocolli comuni presenti in rete.

Memorizzazione e collezionamento dei dati di traffico: database SQL, raw files, RRD (Round Robin Database).

Geolocalizzazione degli host e delle comunicazioni di rete.

Utilizzo efficiente dei sistemi multi-core nell'ambito dell'analisi del traffico di rete.

La parte pratica

SNMP: Utilizzo del MIB-II per la realizzazione di semplici strumenti di monitoraggio di apparati.

NetFlow e sFlow: configurazione ed utilizzo sui più comuni apparati di rete (Juniper e Cisco), utilizzo di strumenti open source (ntop e nProbe) per la raccolta, visualizzazione ed analisi dei flussi di rete.

Memorizzazione di grandi moli di dati: DB relazionali vs DB bitmap.

Consolidamento di metriche di traffico nel tempo: RRD.

Analisi approfondita di Wireshark uno strumento avanzato per l'analisi di pacchetti di rete.

Implementazione di semplici programmi basati su libpcap per la cattura dei pacchetti di rete.

Obiettivi

A conclusione del corso i partecipanti saranno in grado di utilizzare i più comuni strumenti di monitoraggio di rete e di poter utilizzare al meglio i sistemi di analisi del traffico presenti in molti apparati di rete.

Destinatari

Amministratori e tecnici di rete (End-User, Internet Service Provider, rivenditori di apparati e società di consulenza), responsabili e tecnici di Provisioning e Operation.

Prerequisiti

Conoscenze di base di informatica e di networking.



ADSL e Sistemi DSL per non tecnici

Le tecniche xDSL abilitano la trasmissione di segnali digitali ad alta velocità su collegamenti in rame della rete telefonica. Nel corso vengono illustrati gli aspetti tecnici e di servizio dei sistemi xDSL e sono presentate le diverse tecnologie, da quelle simmetriche, quali HDSL e SDSL, a quelle asimmetriche ed in particolare l'ADSL.

Agenda (2 giorni)

La struttura della rete d'accesso telefonica.

Caratteristiche del doppino telefonico.

Sistemi DSL simmetrici: architetture di rete e applicazioni.

Sistemi DSL asimmetrici.

Apparati ADSL

Evoluzione dell'ADSL: ADSL2 e 2+.

Aspetti di provisioning e configurazioni di rete.

VDSL e VDSL 2:

Obiettivi

Presentare la tecnologia dei sistemi xDSL e i servizi che con essi si possono realizzare utilizzando la rete di accesso in rame.

Destinatari

Personale non tecnico.

Prerequisiti

Conoscenze di base sulle reti di TLC.

ADSL e Sistemi DSL: tecnologie e applicazioni

Le tecniche xDSL abilitano la trasmissione di segnali digitali ad alta velocità su collegamenti in rame della rete telefonica. Essi consentono di realizzare collegamenti a larga banda, per la fruizione di servizi multimediali interattivi, riutilizzando l'ultimo tratto della infrastruttura di rete esistente. In tal modo è possibile sfruttare la capillarità di quest'ultima fornendo accessi a larga banda ad un bacino potenzialmente molto vasto di clienti, con investimenti in rete limitati.
Nel corso vengono trattati sia gli aspetti tecnici che di servizio dei sistemi xDSL. Sono illustrate le diverse tecnologie, a partire da quelle simmetriche, quali HDSL e SDSL, principalmente rivolte ad una utenza affari, per poi approfondire quelle asimmetriche ed in particolare l'ADSL. Per ciascuna tecnologia sono descritte le caratteristiche trasmissive e le prestazioni, oltre alle soluzioni architetturali, alle problematiche implementative ed ai servizi supportati. È prevista, inoltre, una breve esercitazione di misura su una linea ADSL, con la interpretazione dei valori che ne risultano per i vari parametri.

Agenda (3 giorni)



Verso la larga banda: i servizi multimediali interattivi.

La struttura della rete d'accesso telefonica.

Caratteristiche del doppino telefonico:

- caratteristiche fisiche (tipi di cavi, struttura dei cavi)
- caratteristiche trasmissive (attenuazione, diafonia).

Sistemi DSL simmetrici: architetture di rete e applicazioni: HDSL e SDSL.

Sistemi DSL asimmetrici:

- le origini della tecnologia ADSL
- allocazione spettrale
- modulazione DMT e aspetti trasmissivi
- schema del collegamento ADSL
- ADSL G.Lite
- stato delle normative.

Apparati ADSL:

- il DSLAM: tipologie e configurazioni
- apparati d'utente.

Evoluzione dell'ADSL: ADSL2 e 2+.

Aspetti di provisioning e configurazioni di rete.

VDSL e VDSL 2: reti di accesso di nuova generazione.

Architetture di rete per servizi su ADSL:

- fast Internet
- Voice over ADSL
- Video over ADSL e IP TV
- Triple Play.

Cenni alle alternative tecnologiche all'ADSL.

Aspetti commerciali.

Esercitazione: misure su una linea ADSL.

Obiettivi

Presentare la tecnologia dei sistemi xDSL e i servizi che con essi si possono realizzare utilizzando la rete di accesso in rame.

Destinatari

Ingegneri di rete e tecnici di operatori di TLC e Service Providers. Tecnici di rete delle aziende manifatturiere di apparati per TLC.

Prerequisiti

Conoscenze di base sulle reti di TLC e sulle tecniche di trasmissione numerica.



Sistemi DSL e Reti a larga banda

La larga banda, vista la crescente necessità di migliorare le prestazioni delle reti per supportare servizi multimediali interattivi, è da diversi anni un tema di grande attualità.
Il corso fornisce una panoramica delle tecnologie e delle architetture per la realizzazione di reti a larga banda che supportino servizi multimediali e convergenti con accesso fisso. Sono brevemente illustrate le tecnologie attualmente in uso per la costruzione di una dorsale (Backbone) multiservizio ad alta capacità, sono indicate le alternative per la rete d'accesso, evidenziandone le differenze tecnologiche e prestazionali. Particolare approfondimento è dato alle tecniche DSL, attualmente le più diffuse per la realizzazione di collegamenti d'accesso ad alta velocità per clientela residenziale e SOHO. Si espongono, poi, le soluzioni in fibra ottica che hanno già trovato ampia diffusione nel sud est asiatico. Si presentano le soluzioni wireless (terrestre, satellitare e mobile), con un confronto delle prestazioni e degli scenari implementativi.

Agenda (3 giorni)

Verso la larga banda

Tecnologie avanzate per Backbone ad alta capacità

- sistemi di trasmissione ad alta velocità sulla lunga distanza
- Backbone IP integrato.

Il problema dell'accesso a larga banda.

La rete di accesso telefonica tradizionale:

- caratteristiche del doppino telefonico e tipologie di cavi
- sistemi DSL simmetrici: HDSL, SHDSL e evoluzioni.

Sistemi ADSL asimmetrici: ADSL.

Aspetti trasmissivi.

Schema del collegamento ADSL.

Architetture di servizio:

- Fast internet
- VoIP
- IP-TV.

Evoluzione dell'ADSL:

- ADSL2/ADSL2+
- il VDSL.

Reti d'accesso in fibra ottica:

- anelli SDH in accesso
- PON (Passive Optical Network)
- soluzioni metro Ethernet
- stato dell'arte.

Tecniche d'accesso via radio: WLL e Wi-Max.

Cenni alle tecnologie via satellite.

Cenni alle tecnologie di trasmissione dati a larga banda mobili: HSPA e LTE.

Obiettivi

Alla fine del corso i partecipanti hanno una conoscenza delle tecnologie e architetture per la realizzazione di reti a larga banda.

Destinatari

Ingegneri di rete e tecnici di operatori di TLC e Service Providers. Tecnici di rete delle aziende manifatturiere e aziende installatrici di reti per TLC.

Prerequisiti

Conoscenze di base sulle reti di telecomunicazione e sulle tecniche di trasmissione.



Diagnosi e localizzazione dei guasti nei cavi per TLC in rame

Nel corso sono descritti innanzitutto i tipi di cavi in rame utilizzati nella rete di TLC, la loro costituzione e i relativi parametri trasmissivi. Sono quindi presentati i principali metodi di misura per la caratterizzazione dei cavi stessi e gli strumenti che possono essere utilizzati. Sono poi approfondite le tecniche di misura ecometriche e quelle basate su ponti resistivi, con sessioni di misura realizzate con strumentazione qualificata, su impianti didattici realizzati con linee artificiali.

Agenda (2 giorni)

Cavi per TLC: tipologia e parametri trasmissivi.

Parametri trasmissivi di un cavo in rame per telecomunicazioni.

Tipi di cavo e loro caratteristiche.

Metodi per la misura dei parametri elettrici e trasmissivi.

Strumenti di misura:

- multimetro
- misuratore di isolamento
- ecometro
- ponte resistivo.

Ecometria ed ecometri:

- principio di funzionamento dell'ecometro
- grandezze fondamentali delle misure ecometriche.
- schema di principio e struttura dell'ecometro
- misure ecometriche
- nozioni complementari sull'uso dell'ecometro
- prove con diverse tipologie di strumenti.

Ponti resistivi:

- criteri generali sulla diagnosi e la localizzazione dei bassi isolamenti
- misure di resistenza
- localizzazione dei guasti con il metodo MURRAY e con il metodo KM
- misure su tratta omogenea, non omogenea, con lunghezza nota
- prove con diverse tipologie di strumenti.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- conoscere la strumentazione di misura per la diagnosi e la localizzazione dei guasti
- saper utilizzare tale strumentazione nelle condizioni tipiche dell'applicazione in campo.

Destinatari

Tecnici di rete di operatori di TLC in particolare addetti all'esercizio e manutenzione della rete. Personale tecnico di aziende installatrici di reti di TLC.

Prerequisiti

Conoscenze di base sull'impiantistica delle reti di TLC.

Misure per la caratterizzazione della linea per sistemi xDSL

Nel corso sono descritti i parametri trasmissivi delle reti in rame, con particolare riferimento al trasporto di segnali numerici in tecnologia xDSL, e le metodologie per la loro rilevazione in impianto. È presentata la strumentazione necessaria e si illustrano le prove necessarie ad ottenere una caratterizzazione completa della linea e delle sue prestazioni.
Le misure descritte sono poi dimostrate con sessioni pratiche svolte, con strumentazione qualificata, su impianti didattici realizzati con linee artificiali.

Agenda (2 giorni)



Cavi per TLC: tipologia e parametri trasmissivi.

Parametri trasmissivi di un cavo in rame per telecomunicazioni.

Tipi di cavo e loro caratteristiche.

Metodi per la misura dei parametri elettrici e trasmissivi.

Strumenti di misura:
- multimetro
- misuratore di isolamento
- ecometro
- ponte resistivo
- esercitazione di misura.

Reti di TLC in rame.

Sistemi xDSL: principio di funzionamento e caratteristiche.

Strumenti di misura.

Misure in corrente continua:
- continuità elettrica dei conduttori costituenti la coppia
- tensione a/b, a/terra, b/terra
- isolamento a/b, a/terra, b/terra
- resistenza rame del doppino
- capacità
- esercitazione di misura.

Misure in alta frequenza (nella banda di interesse):
- capacità mutua a 1 kHz
- attenuazione d'inserzione, di riflessione, di bilanciamento
- rumore di linea, rumore impulsivo, immunità al rumore
- densità spettrale di potenza, paradiafonia, telediafonia
- valutazione del bit rate e del numero di bit per sottoportante (ADSL)
- rilevazione delle microinterruzioni
- esercitazione di misura.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:
- conoscere la strumentazione di misura per la caratterizzazione di una linea xDSL
- saper utilizzare tale strumentazione nelle condizioni tipiche dell'applicazione in campo.

Destinatari

Tecnici di rete di operatori di TLC in particolare addetti all'esercizio e manutenzione della rete. Personale tecnico di aziende installatrici di reti di TLC.

Prerequisiti

Conoscenze di base sull'impiantistica delle reti di TLC e sui sistemi trasmissivi digitali.

Sviluppo della rete di accesso in fibra ottica NGAN (New Generation Access Network)

Lo sviluppo di una nuova rete di accesso (NGAN, Next Generation Access Network), basata sulla fibra ottica, può essere realizzato con soluzioni di vario tipo (FTTx), con collegamenti in fibra fino all'armadio (FTTC) o fino all'edificio (FTTB) o direttamente fino all'abitazione (FTTH).
Nel caso di rete FTTH, inoltre, possono essere sviluppate reti con topologia punto-multipunto (GPON) o punto-punto (P2P).
Il corso – finalizzato alla formazione del progettista – illustra le varie architetture ed approfondisce gli aspetti inerenti la progettazione della rete di accesso nei vari casi, evidenziando i vantaggi e gli svantaggi delle varie soluzioni.
Viene infine approfondito lo standard GPON (ITU-T G.984), che è quello maggiormente impiegato a livello internazionale e vengono descritte le sue possibili evoluzioni: la GPON Staking, per la condivisione della stessa rete tra più Operatori; la NG-PON1 (con tecnologia TDM) e la NG-PON2 (con tecnologia WDM) finalizzate all'incremento delle prestazioni di banda.

Agenda (5 giorni)

Rete in rame:

- descrizione della rete in rame e dei sistemi numerici di piccola (PG) e grande (DLC) capacità
- Local Loop Unbundling (LLU) per la condivisione della rete tra Operatori
- tipi di posa dei cavi (aerea su pali o edifici, sotterranea in trincea, in tubazione e in tubi interrati)
- criteri di sviluppo della rete.

Rete ottica FTTO:

- descrizione dei primi sviluppi della rete ottica di accesso
- criteri di sviluppo della rete ottica FTTO
- evoluzione delle tecniche di realizzazione degli impianti.

Architetture di rete FTTx:

- descrizione e confronto delle possibili architetture FTTx
- criteri di sviluppo della rete FTTB
- il cablaggio degli edifici.

Architetture di rete FTTH:

- descrizione e confronto delle architetture GPON (splitter distribuiti e splitter concentrati) e P2P
- criteri di sviluppo della rete GPON
- criteri di sviluppo della rete P2P.

Rete GPON e sue evoluzioni:

- descrizione della rete GPON (raccomandazione ITU-T G.984)
- descrizione della rete GPON Staking
- evoluzione NG-PON1 (raccomandazione ITU-T G.987) e NG-PON2 (WDM-PON).

Obiettivi

Fornire le conoscenze e i criteri di base per il progetto della rete di accesso in fibra ottica, con specifico riferimento alle topologie FTTB, FTTH-P2P e FTTH-GPON.

Destinatari

Ingegneri di rete e tecnici di operatori di TLC e Service Providers. Tecnici di rete delle aziende manifatturiere e aziende installatrici di reti per TLC.

Prerequisiti

Conoscenza di base sulle reti di TLC.



NGAN (New Generation Access Network)

Lo sviluppo di una nuova rete di accesso (NGAN, Next Generation Access Network), basata sulla fibra ottica, può essere realizzato con soluzioni di vario tipo (FTTx), con collegamenti in fibra fino all'armadio (FTTC) o fino all'edificio (FTTB) o direttamente fino all'abitazione (FTTH).
Nel caso di rete FTTH, inoltre, possono essere sviluppate reti con topologia punto-multipunto (P2MP) o punto-punto (P2P).
Il corso illustra le varie architetture e approfondisce gli aspetti inerenti la progettazione della rete di accesso nei vari casi, evidenziando i vantaggi e gli svantaggi delle varie soluzioni.

Agenda (3 giorni)

Descrizione della Rete di accesso di nuova generazione

- cenni alla rete di accesso tradizionale
- descrizione e confronto delle possibili architetture FTTx (FTTC, FTTB, FTTH)
- criteri di sviluppo e confronto di reti P2P (GBE) e P2MP (GPON)
- standard riferiti alla GPON e loro evoluzione
- criteri di sviluppo e confronto di reti GPON con splitter distribuiti e concentrati
- confronto sistemi PON: BPON, GPON, EPON.

Progettazione della Rete di accesso di nuova generazione

- definizione dell'architettura della rete
- progettazione della rete nei vari casi di architetture FTTH
- il cablaggio degli edifici.

Obiettivi

Fornire le conoscenze e i criteri di base per la progettazione della rete di accesso in fibra ottica, con specifico riferimento alle topologie FTTC, FTTB, FTTH (P2P e P2MP).

Destinatari

Ingegneri di rete e tecnici di operatori di TLC e Service Providers. Tecnici di rete delle aziende manifatturiere e aziende installatrici di reti per TLC.

Prerequisiti

Conoscenza di base sulle reti di TLC.



Architettura UNIX ed ambiente utente

La famiglia dei sistemi operativi UNIX si adatta ad un'ampia gamma di elaboratori ed è largamente impiegata per la sua versatilità e le sue prestazioni. UNIX può essere attualmente considerato, e lo sarà ancora di più in un prossimo futuro, uno standard nel segmento di mercato delle Workstation, dei minicomputer e dei server di rete. Il corso, rivolto agli utenti del sistema operativo UNIX, è propedeutico a tutti quelli relativi a questo sistema. Fornisce i principi fondamentali dell'architettura UNIX, le modalità d'uso e le procedure per la gestione dei servizi offerti. Sono inoltre presentati i principali servizi di rete e gli strumenti di base per lo sviluppo del software.
Il corso è quindi rivolto a coloro che sono interessati all'utilizzo di UNIX, sia come potente ambiente per lo sviluppo del software, che come macchina server per l'esecuzione delle applicazioni aziendali. L'amministrazione del sistema è affrontata per gli aspetti che più da vicino riguardano l'utente, mentre quelli più specialistici sono trattati in altri corsi.

Agenda (5 giorni)



Introduzione all'uso di una macchina Unix:
- file system e meccanismi di protezione
- il terminale virtuale X (X-Window) e la GUI
- editor vi e editor grafici.

L'interprete di comandi (Shell, Cshell ed altri):
- redirezione e pipe
- l'interprete Shell: variabili, parametri e strutture di controllo
- le principali caratteristiche di Cshell: history, aliases e job control.

Amministrazione:
- procedure per il salvataggio e la gestione della memoria di massa
- gestione utenti e gruppi.

UNIX in rete:
- cenni sulla rete Internet
- i servizi di rete (telnet, ftp, mail, WWW, ecc.).

Architettura del sistema operativo e tool per lo sviluppo del software:
- caratteristiche generali del linguaggio C
- struttura del file system e gestione dei processi
- i principali strumenti di sviluppo: cc, lint, debugger, ar, make e sccs
- strumenti per il rapido prototyping: sed, awk, lex, yacc.

Obiettivi

Il corso fornisce ai partecipanti le conoscenze e le competenze necessarie su:
- architettura del sistema operativo UNIX
- ambiente utente.

Destinatari

Sistemisti e sviluppatori che devono acquisire le conoscenze dell'ambiente UNIX.

Prerequisiti

Conoscenza generale dei sistemi di elaborazione e dei sistemi operativi.



La gestione di un server UNIX su una rete IP

Il System Administrator di UNIX deve saper risolvere una serie di problemi che richiedono la conoscenza dell'architettura del sistema. Anche se le ultime versioni del sistema operativo hanno reso l'interfaccia utente più amichevole e prevedono strumenti evoluti di gestione delle risorse hardware e software, le competenze richieste all'amministratore continuano a rimanere elevate, vista anche l'eterogeneità di questi strumenti tra le diverse piattaforme.
Inoltre, le difficoltà legate alla gestione di una macchina UNIX aumentano se il sistema viene inserito su una rete TCP/IP, anche se esiste uno stretto legame tra l'architettura Internet ed il sistema operativo UNIX, che è stato, fin dall'inizio, l'ambiente più naturale per lo sviluppo dei servizi basati su TCP/IP.
Il corso fornisce le conoscenze di base sull'uso degli strumenti che consentono l'installazione, la gestione e la riconfigurazione dei sistemi UNIX, sia stand-alone, che connessi in rete (LAN e WAN). Sono inoltre indicati i metodi e gli strumenti che consentono il corretto "tuning" del sistema e della rete.

Agenda (5 giorni)



L'amministrazione del sistema UNIX Stand Alone:
- installazione e riconfigurazione del kernel
- struttura e gestione dei file system
- procedure di start-up e shutdown, gestione utenti
- accounting, salvataggio archivi, spooling system.

L'amministrazione di un server UNIX in rete:
- richiami sull'architettura Internet e sui principali servizi
- installazione di server UNIX in rete
- routing IP e demoni
- configurazione DNS
- configurazione e struttura dei Mail Exchanger
- configurazione server POP3
- creazione e gestione di un server pubblico (anonymous ftp)
- configurazione server httpd
- diagnostica di reti, sniffing.

Cenni sulla sicurezza del sistema e della rete.

Monitoraggio e tuning del sistema.

Obiettivi

Il corso fornisce ai partecipanti le conoscenze e le competenze necessarie per:
- gestire un server UNIX in una rete TCP/IP
- installare e configurare i principali servizi di rete, Intranet ed Internet.

Destinatari

System Administrator UNIX.

Prerequisiti

Conoscenza di UNIX, almeno a livello utente.

Linux System & Network Administration

Il corso trasferisce le competenze necessarie per installare, configurare e gestire una macchina Linux in una rete TCP/IP nella quale il sistema svolge le funzioni di network server. Il corso parte dall'amministrazione del sistema stand-alone per poi passare all'inserimento del sistema in rete e alla gestione dei servizi di rete. Sia per la parte stand alone sia per la parte network administration particolare attenzione viene posta nella gestione della sicurezza. Il corso fornisce gli strumenti necessari per amministrare autonomamente un sistema Linux in una rete TCP/IP con la possibilità di integrare in essa risorse di sistemi Windows.

Agenda (5 giorni)



Architettura Linux e versioni:

- versioni Linux; struttura del Kernel; struttura e gestione dei file system.

Installazione:

- procedura di installazione; strategie di partizionamento; riconoscimento dell'hardware; configurazione e compilazione del kernel.

Gestione del kernel e dei moduli:

- architettura modulare; comandi lsmod, rmmod, depmod, modprobe; file di configurazione dei moduli; configurazione e ricompilazione.

Boot del sistema:

- impostazioni dei bootloader (LILO, GRUB); parametri di avvio; il sistema dei runlevel di System V.

Amministrazione del sistema:

- i sistemi di gestione dei pacchetti (RPM - Red Hat Package Manager, APT - Advanced Package Tool); programmazione di job periodici; gestione di utenti e gruppi; procedure di backup; hardware; stampanti; gestione dei file di log; gestione crash.

Gestione di file system e partizioni:

- creazione, modifica e ridimensionamento delle partizioni; caratteristiche dei vari file system; creazione, riparazione e ridimensionamento di un file system; configurazione dispositivi RAID.

Amministrazione in rete TCP/IP:

- richiami sul TCP/IP
- configurazione schede di rete
- configurazione server DHCP
- configurazione della rete: router, routing statico
- configurazione dei servizi e xinetd
- DNS (Domain Name System)
- posta elettronica (postfix, POP3, IMAP)
- web server Apache
- condivisione risorse con NFS e Samba
- gestione centralizzata delle utenze: il servizio NIS.

Obiettivi

Al termine del corso i partecipanti hanno le conoscenze e le competenze per:

- eseguire le attività base di amministrazione di sistema
- installare pacchetti software, gestire file system, avviare e fermare il sistema
- amministrare gli utenti e la sicurezza della macchina, gestire le stampanti di rete, gestire i processi di sistema
- configurare e installare i servizi di rete (posta elettronica, DNS, web server,NFS), integrare le reti Windows con Samba.

Destinatari

System Administrator Linux/UNIX.

Prerequisiti

Conoscenza di UNIX, almeno a livello utente.



Microsoft Windows 8

I sistemi operativi della famiglia Microsoft si sono diffusi sempre di più nell'ambito delle realtà aziendali come piattaforme di base per la produttività individuale (l'office automation) e come piattaforme avanzate per il networking e la fornitura di servizi internet (DBMS, WEB server, proxy, cluster, ambienti virtuali etc.). Windows 8 è l'ultima suite di sistemi operativi realizzati dalla Microsoft, destinata ad essere utilizzata sia nell'ambito dell'home computing, che in realtà aziendali come Workstation. Le caratteristiche di sicurezza, affidabilità, prestazioni e semplicità d'uso la rendono piattaforma di riferimento nell'ambito dell'universo Microsoft.
Corso valido per la preparazione all'esame di certificazione 70-687 e il conseguimento della certificazione MCSA.

Agenda (5 giorni)





Installing Windows 8:

- Introducing Windows 8
- preparing to Install Windows 8
- installing Windows 8
- automating the Installation of Windows 8
- activating Windows 8.

Upgrading and Migrating to Windows 8:

- upgrading to Windows 8
- migrating to Windows 8
- migrating User Data and Settings.

Managing Disks and Device Drivers:

- managing Disks, Partitions, and Volumes
- maintaining Disks, Partitions, and Volumes
- working with Virtual Hard Disks
- installing and Configuring Device Drivers.

Configuring and Troubleshooting Network Connections:

- configuring IPv4 Network Connectivity
- configuring IPv6 Network Connectivity
- implementing Automatic IP Address Allocation
- implementing Name Resolution
- troubleshooting Network Connectivity.

Implementing Wireless Network Connections:

- overview of Wireless Networks
- implementing a Wireless Network.

Implementing Network Security:

- overview of Threats to Network Security
- configuring Windows Firewall
- securing Network Traffic
- configuring Windows Defender.

Configuring File Access and Printers on Windows 8 Clients:

- managing File Access
- managing Shared Folders
- configuring File Compression
- managing Printers
- overview of SkyDrive.

Securing Windows 8 Desktops:

- authentication and Authorization in Windows 8
- implementing GPOs
- securing Data with EFS and BitLocker
- configuring User Account Control.

Microsoft Windows 8

Configuring Applications:
- install and Configure Applications
- managing Apps from the Windows Store
- configuring Internet Explorer Settings
- configuring Application Restrictions in the Enterprise.

Optimizing and Maintaining Windows 8 Client Computers:
- optimizing the Performance of Windows 8
- managing the Reliability of Windows 8
- managing Windows 8 Updates.

Configuring Mobile Computing and Remote Access:
- configuring Mobile Computers and Device Settings
- configuring VPN Access
- configuring Remote Desktop and Remote Assistance
- overview of DirectAccess.

Implementing Hyper-V:
- overview of Hyper-V
- creating Virtual Machines
- managing Virtual Hard Disks
- managing Snapshots.

Troubleshooting and Recovering Windows 8:
- backing Up and Restoring Files in Windows 8
- recovery Options in Windows 8.

Using Windows PowerShell:
- introduction to Windows PowerShell 3.0
- windows PowerShell Remoting
- using Windows PowerShell Cmdlets.

Obiettivi

Il corso fornisce le conoscenze e le competenze necessarie per:
- effettuare installazioni ed aggiornamenti a Windows 8
- configurare e gestire le periferiche di sistema, l'ambiente utente, le impostazioni e i protocolli di rete
- lavorare con le nuove tecnologie previste in Windows 8.

Destinatari

System Administrator e professionisti IT che configurano e supportano dispositivi Windows 8 in ambiente workgroup o enterprise.

Prerequisiti

Conoscenza generale di Windows XP/Vista/7, dei protocolli TCP/IP UDP, di Active Directory Domain Services e dei componenti di Windows Automated Installation Kit (WAIK).



Microsoft Windows 2012

Windows Server 2008 ha introdotto, rispetto a i suoi predecessori, una serie di servizi e strumenti che semplificano la realizzazione di reti aziendali distribuite e ne migliorano la sicurezza. La versione 2012 ne migliora ed estende le caratteristiche. Il corso intende fornire ai partecipanti conoscenze sulla organizzazione, la gestione, la configurazione e le attività di un server e tutto ciò che occorre per progettare ed installare una infrastruttura Active Directory Domain Services. Il corso è rivolto a coloro che vogliono usare Windows 2012 per fornire servizi avanzati di networking, servizi aziendali (web e database), per creare una infrastruttura di rete aziendale basata su Windows 2012 o per fornire una piattaforma di virtualizzazione basata su Hyper-V.
Corso valido per la preparazione all'esame di certificazione 70-410 e il conseguimento della certificazione MCSA MCSE ed MCSM.

Agenda (5 giorni)





Deploying and Managing Windows Server 2012:

- Windows Server 2012 Overview
- overview of Windows Server 2012 Management
- installing Windows Server 2012
- post-Installation Configuration of Windows Server 2012
- introduction to Windows PowerShell.

Introduction to Active Directory Domain Services:

- overview of AD DS
- overview of Domain Controllers
- installing a Domain Controller.

Managing Active Directory Domain Services Objects:

- managing User Accounts
- managing Group Accounts
- managing Computer Accounts
- delegating Administration.

Automating Active Directory Domain Services Administration:

- using Command-line Tools for Administration
- using Windows PowerShell for Administration
- performing Bulk Operations with Windows PowerShell.

Implementing IPv4:

- overview of TCP/IP
- understanding IPv4 Addressing
- subnetting and Supernetting
- configuring and Troubleshooting IPv4.

Implementing DHCP:

- installing a DHCP Server Role
- configuring DHCP Scopes
- managing a DHCP Database
- securing and Monitoring DHCP.

Implementing DNS:

- name Resolution for Windows Client and Servers
- installing and Managing a DNS Server
- managing DNS Zones.

Implementing IPv6:

- Overview of IPv6
- IPv6 Addressing
- Coexistence with IPv6
- IPv6 Transition Technologies.

Microsoft Windows 2012

Implementing Local Storage:
- overview of Storage
- managing Disks and Volumes
- implementing Storage Spaces.

Implementing File and Print Services:
- securing Files and Folders
- protecting Shared Files and Folders Using Shadow Copies
- configuring Network Printing.

Implementing Group Policy:
- overview of Group Policy
- Group Policy Processing
- implementing a Central Store for Administrative Templates.

Securing Windows Servers Using Group Policy Objects:
- Windows Security Overview
- configuring Security Settings
- restricting Software
- configuring Windows Firewall with Advanced Security.

Implementing Server Virtualization with Hyper-V:
- overview of Virtualization Technologies
- implementing Hyper-V
- managing Virtual Machine Storage
- managing Virtual Networks.

Obiettivi

Il corso fornisce le conoscenze e le competenze necessarie per:
- analizzare le principali caratteristiche e servizi della piattaforma di rete Windows
- pianificare ed installare Windows Server 2012
- installare e configurare i principali servizi di rete, Intranet ed Internet
- configurare una infrastruttura Active Directory
- analizzare le nuove tecnologie per l'accesso remoto
- installare e configurare le tecnologie di virtualizzazione Hyper-V.

Destinatari

System Administrator e quanti operano nel supporto tecnico.

Prerequisiti

Conoscenza dei sistemi operativi e dei servizi di rete, familiarità con Windows Server 2003/2008.



Windows 8/2012: amministrazione remota e scripting

Il corso fornisce agli amministratori dei sistemi operativi Microsoft, da Windows XP/2003 a Windows 8/2012, le conoscenze necessarie per sfruttare al meglio Powershell, Windows Script Host (VBScript), Windows Management Instrumentation (WMI) e componenti COM per amministrare da remoto una infrastruttura di rete. Offre una panoramica delle altre tecnologie utilizzabili per amministrare da remoto un ambiente Windows: servizi per la gestione remota, tools a riga di comando del sistema operativo e tools avanzati del Resource Kit.

Agenda (3 giorni)



Servizi utilizzati all'interno di una LAN.

Panoramica delle tecnologie di scripting per Windows:

- Batch
- VBScript
- PowerShell.

Utilizzo di oggetti.

Interazione degli script con i componenti COM.

Logica degli script.

Debug e gestione degli errori.

ADSI: nozioni di base.

Creazione di script di accesso.

Script di amministrazione.

Funzioni avanzate (WMI).

Nozioni di base sull' interazione con Database (ADO).

Eseguibili utilizzabili da prompt dei comandi o Telnet.

Analisi dei tools del Resource Kit per amministrare i sistemi Windows.

Programmazione batch utilizzando i comandi esposti.

Accesso remoto ad una intranet (VPN, DirectAccess) e gestione di un sistema da remoto.

Analisi dei Terminal Services per l'amministrazione remota.

Obiettivi

Il corso fornisce le conoscenze e le competenze necessarie per:

- utilizzare i principali strumenti di gestione remota
- analizzare le tecniche di scripting mediante Command, VBScript e PowerShell
- sviluppare semplici script per la gestione di reti basate su Windows.

Destinatari

System Administrator e quanti operano nel supporto tecnico.

Prerequisiti

Conoscenze di base sullo scripting ed esperienza nell'utilizzo e amministrazione di: Server Windows 2003/2008/2012, servizi di Active Directory, servizi di rete e gestione dei sistemi.



Windows/Unix:interoperabilità dei servizi di rete

Il corso trasferisce le competenze di base per selezionare, progettare e implementare i servizi di rete presenti in una LAN utilizzando Microsoft Windows e la piattaforma Unix/Linux. Sono presentate le soluzioni tecnologiche offerte dai due sistemi, mettendoli a confronto in una situazione reale aziendale ed analizzandone caratteristiche e problematiche principali.

Agenda (3 giorni)

Servizi utilizzati all'interno di una LAN.

Servizi indispensabili per la visibilità su Internet.

Assegnazione statica e dinamica degli indirizzi.

Risoluzione dei nomi computer su LAN.

Gestione e cooperazione di DNS e DHCP.

File sharing e Print services.

Gestione centralizzata delle risorse di rete.

Analisi comparative delle soluzioni e premesse per l'utilizzo del servizio LDAP.

Evoluzione verso il database integrato.

Interoperabilità delle applicazioni: Wine e SUA.

Esecuzione contemporanea dei sistemi operativi mediante virtualizzazione: VMWARE, Hyper-V, VirtualBox.

Scenario finale sulla gestione dei servizi di rete.

Obiettivi

Il corso si propone di trasmettere ai partecipanti le conoscenze e le competenze necessarie per:

- analizzare le caratteristiche dei servizi di rete delle piattaforme Windows e Unix
- individuare le problematiche di coesistenza/cooperazione dei due Sistemi Operativi e le possibili soluzioni
- progettare una semplice infrastruttura di rete mista Windows/Unix.

Destinatari

System Administrator e responsabili IT.

Prerequisiti

Per trarre pieno beneficio dal corso, è richiesta una conoscenza generale dei sistemi operativi e dei servizi di rete.



One Page Project Map

Organizzare le risorse e le attività in funzione di un obiettivo è una competenza di base che serve a tutti, non solo agli specialisti. Le cose fondamentali si possono imparare in una giornata, ma è soprattutto utile mettere in comune in comune alcune definizioni in modo da avere un linguaggio condiviso e potente nel fare accadere le cose.

Agenda (1 giorno + 2 settimane di tutoring on line + 1 giorno)





Il vostro lavoro: Come vi organizzate ? Cosa funziona ?

Quali ostacoli ?

Cosa dovete fare nel prossimo futuro ? (attività facilitata da cui emergono i “progetti” per la parte pratica della giornata).

Alcune definizioni: Progetto, Risultato, Qualità, Responsabilità.

Le routine base del project management: scoping, planning, avanzamento lavori, chiusura.

Presentazione One Page Project Map ™ ed applicazione guidata.

Project Work (sulle attività emerse al mattino o su progetti già in corso o da avviare portati dai partecipanti che saranno istruiti in tal senso nell’invito al corso).

Obiettivi

Al termine di questo corso i partecipanti saranno in grado di:

- dare una definizione (condivisa) di progetto, risultato, qualità, responsabilità
- applicare la metodologia One Page Project Map ™ al proprio contesto di lavoro riconoscendo le situazioni critiche e adattandola ove necessario
- riconoscere i limiti dell’ambito di applicazione e come relazionarsi a contesti dove sia opportuno ricorrere ad una organizzazione di progetto più elaborata

Destinatari

Tutti i livelli.

Prerequisiti

Nessuno.



Basics di Project management

Il successo dei progetti ICT dipende dalla capacità di tutti i membri del gruppo di progetto di fornire, oltre al contributo specialistico, anche un contributo gestionale che prevede sia un coinvolgimento per stilare un piano di progetto realizzabile sia un coinvolgimento per produrre lo stato di avanzamento del progetto. ***I contenuti del corso sono in linea con gli standard di Project Management sviluppati dal Project Management Institute (PMI).***

Agenda (3 giorni)

Processi, programmi e progetti

Il project management:

- logiche e strumenti
- i ruoli e la motivazione nella gestione dei progetti
- il ciclo di vita dei progetti
- il sistema degli stakholder e la sua gestione.

La garanzia del rispetto dei tempi e gli strumenti di pianificazione, programmazione e controllo:

- la WBS (Work Breakdown Structure)
- la matrice Attività-Responsabilità
- le tecniche reticolari di gestione dei progetti il diagramma di GANTT, il PERT, il CPM.

Il piano dei costi:

- il controllo di gestione del progetto
- il budget di progetto
- la curva ad S
- il PERT costi.

Il controllo degli stati di avanzamento del progetto.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- contribuire in maniera professionale alla definizione del piano dei tempi e dei costi del progetto
- migliorare la capacità di fornire il loro contributo gestionale al capo progetto.

Destinatari

Quanti partecipano al gruppo di lavoro per la gestione dei progetti.

Prerequisiti

Nessuno.



Microsoft Project - Base

Il Project Management è la disciplina che consente di gestire efficacemente un progetto rispettando i vincoli che a volte possono essere anche rigidi. Approcciare il progetto con una metodologia appropriata e usare uno strumento informatico adeguato migliorano la probabilità di raggiungere gli obiettivi stabiliti dagli stakeholder.
Supportare le attività di Pianificazione e Controllo dei progetti con applicazioni software dedicate consente infatti: forte riduzione dei tempi di impostazione dei piani, maggior precisione nelle previsioni e nei consuntivi, possibilità di effettuare simulazioni durante l'intero ciclo di vita del progetto, così da garantire il governo dei processi decisionali per raggiungere gli obiettivi tempi/costi/qualità e la disponibilità di output utili ai vari tipi di comunicazioni.
Il corso prepara a gestire in modo adeguato la grande quantità di dati che un progetto richiede e produce.

Agenda (2 giorni)



Elementi caratteristici dell'applicazione: tabelle, gantt, moduli, barra di project, barre degli strumenti.

Pianificazione del progetto:

- definizione di calendari
- inserimento WBS, attività e informazioni personalizzate utente
- produzione Gantt e personalizzazione con definizione del tipo attività (durata fissa, unità fissa, lavoro fisso)
- produzione network e personalizzazione
- definizione e gestione dei vincoli rigidi e flessibili
- definizione delle informazioni caratterizzanti le risorse, tipologie e loro assegnazioni alle attività di progetto
- livellamento delle risorse per una distribuzione ottimale dei carichi di lavoro
- definizione e allocazione dei costi di progetto
- analisi delle informazioni di pianificazione del progetto ai fini dell'approvazione delle baseline
- determinazione e consolidamento delle baseline di progetto
- dati current, actual e planned gestiti da MS Project.

Controllo del progetto:

- definizione del timenow di progetto
- descrizione degli elementi caratteristici dell'applicazione ai fini di un corretto aggiornamento dei dati di progetto
- inserimento dei dati effettivi (tempi, risorse e costi)
- determinazione del forecast di progetto
- determinazione dei parametri di scostamento secondo l'Earned Value Method
- gestione del versioning delle baseline e re-baseline di progetto.

Obiettivi

Consentire ai partecipanti di:

- definire la WBS e le attività di progetto
- creare e gestire il network di progetto
- assegnare le risorse e definire i carichi ottimali
- definire i costi di progetto
- aggiornare il progetto con i dati effettivi per monitorare e controllare il progetto
- gestire le comunicazioni con gli stakeholder.

Destinatari

Responsabili e Professional che hanno l'esigenza di utilizzare strumenti base per il PM.

Prerequisiti

Metodi e tecniche di Project Management.



Microsoft Project - Avanzato

Il Project Management è la disciplina che consente di gestire efficacemente un progetto rispettando i vincoli posti dagli stakeholder. L'uso di meccanismi e una metodologia appropriata, affiancata ad uno strumento informatico adeguato, consentono non solo di aumentare la probabilità di successo del progetto, ma anche di rendere più efficiente ed efficace il lavoro di chi gestisce il progetto stesso. Questo corso consente ai partecipanti di produrre pianificazioni avanzate e fare analisi sui dati di progetto in modo da evidenziare rapidamente e tempestivamente le situazioni di criticità.

Agenda (2 giorni)



Definizione di modelli per realizzare rapidamente la pianificazione partendo da progetti già conclusi con successo.

Creazione e gestione dei filtri e raggruppamenti di dati personalizzati dagli utenti.

Definizione di report di sintesi e grafici di cruscotti gestionali con indicatori di "tipo semaforico".

Definizione di strutture di progetto che permettano di aggregare dati su risorse o attività al fine di analizzare con maggiore cura l'impegno delle risorse coinvolte nel progetto.

Definizione e gestione di un team di risorse condivise tra più progetti.

Definizione e gestione di un portfolio/programma di progetti.

Obiettivi

Consentire ai partecipanti di:

- definire la WBS e le attività di progetto
- creare e gestire il network di progetto
- assegnare le risorse e definire i carichi ottimali
- definire i costi di progetto
- aggiornare il progetto con i dati effettivi per monitorare e controllare il progetto
- gestire le comunicazioni con gli stakeholder.

Destinatari

Responsabili e professional che hanno l'esigenza di utilizzare strumenti avanzati per il PM.

Prerequisiti

Conoscenze di base di Ms Project.



Lavorare per progetti

Le imprese nel rispondere alle molteplici sollecitazioni ambientali, tendono ad accentuare la flessibilità e ad innovare processi, strutture, prodotti e servizi. Ciò richiede di affrontare problemi complessi e di adottare soluzioni organizzative che si integrino nelle strutture dell'organizzazione permanente. A questo ordine di problematiche dà il suo contributo solutivo la "gestione per progetti" che può interessare, ad esempio, i progetti organizzativi, informatici o formativi e la gestione di programmi aziendali di ricerca e di sviluppo di nuovi prodotti. Il successo di un progetto dipende dalle capacità del Project Manager e dei responsabili di sottoprogetti o di task di capire i bisogni del cliente e di tutti gli stakeholder di progetto, di pianificare e controllare le attività da svolgere ed i costi correlati, di coinvolgere persone diverse che non appartengono in generale alla stessa funzione aziendale, di comunicare e di negoziare nell'ambiente di progetto. In linea con questo principio il percorso formativo offre la possibilità di affrontare in maniera integrata da una parte le metodologie e le tecniche per organizzare e controllare un progetto con particolare attenzione ai risultati in termini di costo/tempi/qualità, e dall'altra gli aspetti relazionali legati alla gestione dei gruppi di progetto.
Il corso, in linea con gli standard di Project Management sviluppati dal Project Management Institute (PMI), fornisce le competenze necessarie per sostenere l'esame di certificazione PMP e CAPM.

Agenda (3+2 giorni)



Parte I (3 giorni)

Processi, programmi e progetti. Il project management.

La garanzia del rispetto dei tempi e gli strumenti di pianificazione, programmazione e controllo:
- la WBS (Work Breakdown Structure)
- la matrice Attivita-Responsabilità
- le tecniche reticolari di gestione dei progetti il diagramma di GANTT, il PERT, il CPM.

I sistemi informativi di supporto alla gestione dei progetti: Microsoft Project.

Elementi relativi alla gestione della qualità e degli approvvigionamenti.

Il controllo dei costi:
- il controllo di gestione del progetto
- il budget di progetto
- la curva ad S e il PERT costi.

Il metodo earned value per il controllo incrociato dei costi e dei tempi.

Parte II (2 giorni)

La gestione del gruppo di progetto:
- il funzionamento del gruppo di progetto e la gestione delle riunioni
- i ruoli nel gruppo di progetto: capo progetto, specialisti, rappresentanti cliente, terze parti
- le decisioni nel gruppo di progetto: decision checking, decision making, decision taking, decision acting
- le tecniche di problem solving.

La negoziazione nel gruppo di progetto.

Obiettivi

Far acquisire:
- metodologie e tecniche relative all'articolazione del progetto, alla gestione dei parametri strategici, alla programmazione ed al controllo, ai sistemi informativi di supporto
- consapevolezza relativa ai fenomeni legati ai gruppi di progetto per migliorare la capacità di gestione.

Destinatari

Project Manager e Professional che operano su progetti.

Prerequisiti

Nessuno.



La gestione dei progetti ICT

Il corso affronta le problematiche organizzative e gestionali di un progetto ICT rispetto a due direttrici principali: la gestione delle persone all'interno del gruppo di lavoro e la gestione organizzativa di progetti complessi all'interno dell'azienda. Per affrontarli con efficacia, il capo progetto deve attivare relazioni adatte con il management (sponsor dell'iniziativa), il cliente e con gli utenti, gestire il budget e gli aspetti qualitativi, la dimensione multi progetto, l'insieme delle problematiche contrattuali e, in ultimo, adottare soluzioni organizzative che si integrino nelle strutture dell'organizzazione permanente.
Il corso, in linea con gli standard di Project Management sviluppati dal Project Management Institute (PMI), fornisce le competenze di base necessarie per sostenere l'esame di certificazione PMP e CAPM.

Agenda (3+2 giorni)





Parte I (3 giorni)

Processi, programmi e progetti.

Il project management:

- logiche e strumenti
- i ruoli e la motivazione nella gestione dei progetti
- il ciclo di vita dei progetti
- il sistema degli stakholder e la sua gestione.

Il ciclo di vita del progetto ICT e del prodotto ICT.

L' avvio del progetto ICT - definizione degli obiettivi e redazione del Project Charter.

La pianificazione del progetto ICT:

- la scomposizione del progetto (WBS) e la matrice di assegnazione delle responsabilità (RAM)
- la preparazione del reticolo di progetto: attività, legami e durate
- la Pianificazione del progetto in termini di tempi, risorse e costi
- la Baseline di progetto.

L' esecuzione ed il controllo del progetto ICT.

- gli aggiornamenti e la consuntivazione del progetto: come rilevare gli avanzamenti
- previsioni, stime a finire e analisi degli scostamenti (tecnica dell'Earned Value)
- il documento di avanzamento (SAL).

La chiusura del progetto ICT.

Parte II (2 giorni)

La gestione del gruppo di progetto:

- il funzionamento del gruppo di progetto
- la gestione delle riunioni
- i ruoli nel gruppo di progetto: capo progetto, specialisti, rappresentanti cliente, terze parti
- le decisioni nel gruppo di progetto: decision checking, decision making, decision taking, decision acting
- le tecniche di problem solving.

La negoziazione nel gruppo di progetto.

Obiettivi

Al termine del corso i partecipanti sono in grado di:

- applicare metodologie e tecniche relative all'avvio, la pianificazione, l'esecuzione, il controllo e la chiusura dei progetti
- leggere i fenomeni legati ai gruppi di progetto per migliorare la loro capacità di gestione.

Destinatari

Project Manager e Professional che operano su progetti ICT.

Prerequisiti

Nessuno.



Project Management Professional : Certificazione PMP/PMI®

Il percorso, rivolto a figure con una consolidata esperienza lavorativa nella gestione dei progetti, fornisce le conoscenze necessarie ad affrontare l'esame per l'acquisizione della credenziale PMP®.
L'intervento si articola in una serie di attività da svolgere sia in aula sia fuori, supportato da risorse e servizi prima, durante e dopo il corso, secondo un modello che ha dato negli anni un alto tasso di successo nel superamento degli esami.
Nello specifico l'intervento propone:
lezioni in aula in cui vengono spiegati i processi della Guida al PMBOK® e tutti gli argomenti ricorrenti all'esame PMP/PMI®
accesso all'applicazione web PMTest (www.pmtest.it) per verificare via web l'apprendimento, eseguendo test specifici e simulazioni d'esame;
consulenza sulla redazione della domanda all'esame PMP® e su tutto l'iter previsto dal PMI®.
Sono affrontati anche aspetti non direttamente trattati nel PMBOK®, come il Codice di condotta Etica e Professionale o tecniche di schedulazione dei progetti non tradizionali, che pure sono ricorrenti nelle domande d'esame. A tal riguardo, sono previsti approfondimenti tratti dalla letteratura specializzata suggerita dal PMI®.
Il corso è tenuto da docenti certificati PMP®, con decennale esperienza nel settore del Project Management sia come consulenti su progetti sia come formatori.
Al termine del corso i partecipanti acquisiscono le conoscenze fondamentali per superare l'esame di certificazione professionale PMP®.

Agenda (8 giorni: 2+2+2 giorni + 1+ 1 giorno di simulazione d'esame)





Modulo 1 (2 giorni):
- Introduzione alla Guida al PMBOK®
- Ciclo di vita e organizzazione
- Standard dei processi
- Code of Ethics and Professional Conduct
- Project Integration Management
- Project Scope Management
- Project Time Management.

Modulo 2 (2 giorni):
- Project Cost Management
- Project Quality Management
- Project Human Resource Management.

Modulo 3 (2 giorni):
- Project Communications Management
- Project Risk Management
- Project Procurement Management.

Modulo 4 (1 giorno):
- Simulazione d'esame
- Commento degli errori.

Modulo 5 (1 giorno):
- Simulazione d'esame
- Commento degli errori.

Project Management Professional : Certificazione PMP/PMI®

Obiettivi

Acquisire le conoscenze fondamentali per gestire progetti/programmi.

Destinatari

Project Manager che vogliano certificarsi.

Prerequisiti

Conoscenze di base relative alle metodologie di pianificazione e controllo di progetto.
Ai candidati all'esame PMP® è richiesto il possesso di un'adeguata esperienza gestionale in tema di project management. In particolare:

- i laureati devono possedere almeno 4.500 ore di esperienza realizzata in almeno 3 anni e non oltre i 6 anni antecedenti la domanda d'esame
- i diplomati devono possedere almeno 7.500 ore di esperienza realizzata in almeno 5 anni e non oltre gli 8 anni antecedenti la domanda d'esame.

Personal Training Kit

Ad ogni partecipante verrà rilasciata la seguente documentazione:

- *Libro*: Standard internazionale di project management. Guida alle credenziali CAPM©/PMP© e standard di gestione dei progetti complessi
- *Manuale*: raccolta del materiale utilizzato dal docente in aula
- *Consigli e promemoria*: breve elenco di consigli pratici da attuare per svolgere al meglio l’esame ed elenco di formule, concetti, dati quantitativi e quanto altro necessario da memorizzare per l’esame
- *Supporti per la redazione alla domanda d'esame*: all'avvio del corso saranno consegnati strumenti informatici (file MS Excel) e istruzioni per redigere velocemente l'application form PMI®
- *Accesso all'applicazione PMTest*: quasi 2000 domande disponibili per test e simulazioni d'esame.



La gestione dei rischi e delle opportunità di progetto

La valutazione e la gestione del rischio è parte integrante delle attività di gestione di un progetto e del suo piano: la funzione di presidio dei rischi rappresenta una componente essenziale dell'attività di gestione complessiva e, proprio per questo motivo, non può essere demandata all'estro, alla fantasia, alla buona volontà del singolo Project Manager, ma, al contrario, necessita di un approccio sistematico, che ne assicuri la corretta impostazione, e formalizzato da apposite procedure aziendali che ne garantiscano i corretti canoni di applicazione.
Il ricorso a tecniche e metodologie consolidate e applicate uniformemente da tutte le strutture organizzative aziendali coinvolte, rappresenta una condizione assolutamente necessaria affinché gli sforzi profusi in fase realizzativa si traducano nell'ottenimento di reali vantaggi sul piano della gestione integrata del progetto.

Agenda (3 giorni)

Il rischio di progetto:

- definizione di rischio
- tipologia, natura e origine dei rischi
- processo tecnico di presidio del rischio.

La fase di identificazione:

- analisi della sensitività
- clausole revisione prezzi
- analisi serie storiche
- valore atteso
- analisi del Trend.

La fase di valutazione:

- matrice di esposizione
- soglia di attenzione
- teoria delle decisioni
- Expected Monetary Value
- Decision Trees
- tecniche di simulazione
- Expert Judgements
- scala delle priorità.

Esercitazione.

La fase di pianificazione:

- processo di realizzazione del rischio
- pianificazione iniziale
- il "Risk Plan".

La fase di controllo:

- Check in Progress
- presidio dei rischi
- aggiornamento del Risk Plan.

Obiettivi

Al termine del corso i partecipanti saranno in grado di acquisire:

- la corretta modalità di approccio al processo di gestione dei rischi di progetto
- le metodologie più efficaci per individuare, dimensionare e pianificare i rischi
- le tecniche di supporto da impiegare nelle fasi operative di presidio del rischio.

Destinatari

Manager e Professional che vogliano approfondire le conoscenze sulle tecniche del Risk management.

Prerequisiti

Conoscenze di base relative alle metodologie di pianificazione e controllo di progetto.



Le capacità manageriali del project manager

Coordinare team di progetto richiede capacità manageriali in quanto il Project Manager si trova a gestire, senza avere l'autorità gerarchica, persone di diverse funzioni, unità o professionalità. Il corso consente di ancorare le competenze del proprio ruolo a specifiche soft skills manageriali, sviluppando la leadership necessaria alla creazione e gestione del proprio team di progetto.

Agenda (3 giorni)

Gruppo e gruppo di lavoro:

- ruoli chiave
- organizzare il lavoro
- il processo decisionale del team.

Guidare il team di progetto:

- incoraggiare la partecipazione e la cooperazione
- le regole di comunicazione
- motivare le persone per ottenere il massimo da ognuno
- coniugare gli obiettivi di progetto agli obiettivi individuali.

Il processo di delega:

- gestire il team attraverso la competenza e la fiducia.

Esercitare la propria leadership nel team:

- basi della leadership
- creare consenso
- saper costruire sulle differenze culturali, professionali e metodologiche.

Negoziare efficacemente:

- psicologia ed etica della negoziazione
- tipi di negoziazione
- capacità relazionali e strategiche
- gestire i conflitti.

Obiettivi

Alla fine del corso i partecipanti saranno in grado di:

- gestire persone eterogenee
- gestire le situazioni conflittuali
- motivare e coinvolgere i membri del team verso l’obiettivo comune
- ottenere il massimo dalle potenzialità del gruppo
- gestire le riunioni di progetto
- negoziare per ottenere mezzi e risorse.

Destinatari

Project manager che vogliano migliorare la sfera manageriale del proprio profilo.

Prerequisiti

Conoscenze principali di Project Management.



IT Planning & Programming

Governare efficacemente le risorse IT (Progetti, Processi, Persone, Risultati/KPI) e stare vicino, vicinissimo…. dentro al business portando innovazione "utile".

Agenda (2 giorni)

Il ruolo delle tecnologie e del CIO.

Principi di pianificazione e programmazione. Fattori produttivi dell'IT, cicli di pianificazione, organizzazione del service development e del service delivery, modalità di programmazione delle attività. Paradigmi del project, program e process management.

Demand Management e governo degli investimenti tecnologici (portfolio applicativo, parco hw e sw).

L'IT come driver dell'innovazione e del controllo costi.

Scenari organizzativi e implicazioni sulla pianificazione e programmazione.

KPI e metriche.

Obiettivi

Al termine di questo corso i partecipanti saranno in grado di:

- definire il proprio "ecosistema IT" in termini di risorse, processi, risultati, kpi
- spiegare i processi di Pianificazione annuale e Programmazione mensile o trimestrale di attività, risorse (headcount, vendor, opex, capex)
- identificare le esigenze di processi e tools per il governo dell'IT e per il rilevamento della domanda di servizi e applicazioni in modo che la tecnologia supporti o addirittura guidi il business nell'individuare le migliori opportunità
- discutere diversi scenari organizzativi e definire il fabbisogno di competenze
- individuare i KPI più utili in relazione agli indirizzi strategici aziendali
- spiegare cosa favorisce / ostacola l'innovazione sui servizi e organizzativa.

Destinatari

CIO, PMO, Project Manager area IT, Controller IT, IT Architect

Prerequisiti

Nessuno.



Agile Project Management

Il corso descrive le metodologie per un approccio Agile nella gestione dei progetti, tenendo in considerazione che la gestione deve esaltare la massimizzazione del valore rilasciato in tempi rapidi, la comprensione delle necessità degli stakeholder coinvolti, il coinvolgimento, l'empowerment e la collaborazione del team.

Agenda (2 giorni)



Traditional waterfall projects – SDLC.

Agile manifesto: valori e principi.

Scrum: pilastri, eventi/pratiche, Artefatti, ruoli.

XP: i valori.

Project justification / selection (BCR, payback, NPV, IRR).

Chartering.

Customer-Valued prioritization.

Relative prioritization.

Product roadmap/Story map (Backbone, Walking skeleton).

Risk-adjusted backlog.

Agile contracting.

Task and Kanban board.

Incremental delivery (COC and Plain vanilla version).

Feedback techniques: Prototypes, simulation, demonstrations (IKIWISI).

Cumulative Flow Diagram CFD - Little's law.

Risk burndown chart.

Wireframes.

Story o User story e Backlog.

INVEST criteria e gerarchia dei requisiti.

Information radiators (Visual controls; Information refrigerator).

Burn-down/up chart.

Velocity.

Active listening.

Conflict resolution.

Managership vs Leadership.

Servant leadership model.

Adaptive (situational) leadership: team building phases.

Daily stand-up meeting / Team Space.

Co-located teams (osmotic communication, tacit knowledge, caves and common).

Distribuited teams.

Timeboxing.

Progressive elaboration: rolling wave planning.

Minimally Marketable Feature (MMF).

Estimation (Wideband Delphi, Planning poker, Ideal time).

Relative sizing / Story points (Baseline story, Fibonacci).

Affinity estimating (triangulation).

Release/Iteration planning.

Cycle time, WIP, Throughput.

Escaped defects.

Continuous integration.

Risk-based spike (fast failure, sunk cost).

Retrospective.

Obiettivi

Fornire le metodologie per una gestione del team di progetto che sia adattiva, iterativa e incrementale, basata su differenti livelli di pianificazione, il monitoraggio e la risoluzione dei rischi, il continuous improvement.

Destinatari

Project Manager e Professional che operano su progetti.

Prerequisiti

Nessuno.



Il Mobile Marketing

Il cellulare rappresenta il mezzo di comunicazione che ha registrato gli indici di crescita più consistenti sia in termini di utenze attive, sia dal punto di vista dei servizi utilizzati. La convergenza digitale tra i device e le reti di comunicazione configura la telefonia mobile come il settore potenzialmente di maggiore sviluppo in un ottica di comunicazione multicanale. In questo quadro tecnologico le aziende sono chiamate a prestare un'attenzione sempre più crescente al cellulare come nuovo strumento di Marketing Communication e Advertising. Nuove strategie di comunicazione e di pubblicità stanno caratterizzando il mercato della telefonia mobile; resta in ogni caso da valutare il livello di efficacia e di successo di tali strategie innovative nel Marketing Mix delle aziende, unitamente alle opportunità e ai rischi sottesi.
Il seminario presenta una panoramica sul mercato del Mobile Marketing, con riferimento alle strategie, alle tecniche e agli strumenti più utilizzati dalle aziende italiane e del mercato internazionale; fornisce le chiavi di lettura per valutare le opportunità, i rischi e gli ostacoli della comunicazione aziendale attraverso la telefonia mobile.

Agenda (1 giorno)

Lo scenario della telefonia mobile:

- le generazioni di telefonia cellulare: dall'analogico al digitale always on
- l'evoluzione dei servizi di telefonia mobile
- convergenza Cellulare-PC e Internet Mobile
- i dati sul mercato della telefonia cellulare e dei servizi mobile utilizzati.

Il Mobile Marketing:

- il cellulare come strumento di Marketing Communication
- il Piano di Mobile Marketing: obiettivi, target e prodotti
- le opportunità del Mobile Marketing per le aziende
- i rischi del Mobile Marketing per le aziende.

Le strategie di Mobile Marketing:

- Mobile Corporate Communication
- Mobile Advertising
- Mobile Promotion.

Gli strumenti di Mobile Marketing:

- le strategie multicanali: Cellulare, Internet e TV Digitale
- Display Advertising
- SMS e MMS Advertising
- Bluetooth Marketing
- Advergames on the Mobile Phone.

Il mercato del Mobile Marketing:

- il livello di maturità delle imprese italiane
- i dati sui settori di mercato più attivi nel Mobile Marketing
- le prospettive evolutive.

Obiettivi

Presentare le evoluzioni del settore della telefonia mobile dal punto di vista delle aziende e della comunicazione di marketing e pubblicitaria, con riferimento ai punti di forza e ai punti di debolezza delle strategie di Mobile marketing.

Destinatari

Quanti operano nell'Area Marketing e Comunicazione.

Prerequisiti

Nessuno.



Web 2.0 & Social Networking: scenari e impatti

Lo sviluppo delle tecnologie digitali e dei new media, Internet in testa, ha modificato in tempi rapidi e in modo incisivo le modalità di intendere e gestire sia le logiche di comunicazione e di interazione, sia i processi di costruzione e condivisione della conoscenza. Le tecnologie telematiche sono entrate pervasivamente nella nostra quotidianità, contribuendo a modificare significativamente la struttura della società. Se nella seconda metà degli anni Novanta il Web ha mostrato le sue potenzialità mediatiche e comunicazionali, più di recente lo sviluppo del Web 2.0 e il consolidamento di applicazioni come i Social Network hanno registrato forti ripercussioni in tutti i settori della vita sociale, intervenendo sulle dinamiche relazionali e impattando sui processi di costruzione e di condivisione di saperi e conoscenze.
Il seminario analizza il fenomeno del Web 2.0, con riferimento ad aspetti tecnologici e modelli di servizio; sulla base di tale analisi, passa in rassegna gli impatti del Social Networking sui processi di comunicazione, di interazione e di condivisione di conoscenza.

Agenda (1 giorno)

Lo scenario del Web:

- dalla nascita del www al Web 2.0
- definizione di Web 2.0
- User Generated Content
- decentralizzazione e Long Tail.

Gli strumenti e le tecnologie del Web 2.0:

- Blog
- Wiki
- Social Network
- Podcasting e Vodcasting
- Tagging, Folksonomie e Social Bookmarking
- XML e AJAX.

I modelli di servizio del Web 2.0:

- i design pattern: differenze tra Web 1.0 e Web 2.0
- il Web come piattaforma
- l’architettura partecipativa
- Mashup.

I Social Network Site:

- definizione di Social Network
- l’architettura delle reti sociali
- sei gradi di separazione
- Social Network Analysis
- le tipologie di Social Network.

I nuovi modelli di interazione e conoscenza delle reti sociali:

- dalle reti di interazione ai processi di relazione
- dalla condivisione di informazioni alla costruzione condivisa di conoscenza
- i punti di forza delle reti sociali
- i punti di debolezza delle reti sociali.

Obiettivi

Presentare gli impatti che le applicazioni di Web 2.0 e di Social Networking registrano sulle modalità di comunicazione e di interazione tra gli individui e sui processi di costruzione e condivisione di conoscenza.

Destinatari

Imprenditori e quanti operano nell’Area Marketing e Comunicazione.

Prerequisiti

Nessuno.



Cloud Oriented

Il Cloud Computing rappresenta la più importante transizione nel settore IT dopo l'avvento di Internet. Con il Cloud Computing l'infrastruttura IT diventa un servizio a consumo, come l'elettricità. In questo nuovo paradigma le risorse interne all'azienda saranno dedicate solo alla progettazione, realizzazione e gestione delle applicazioni strategiche. L'infrastruttura si adatterà in tempo reale ai consumi effettivi, non ci saranno più risorse inutilizzate. La ripartizione dei costi fra gli utilizzatori effettivi sarà implicita nel modello e disponibile da subito.
L'unica cosa che ci separa da questo nuovo paradigma ideale e altamente efficiente sono le competenze necessarie per progettare, realizzare e gestire sistemi che traggano il massimo vantaggio dal nuovo paradigma.
Il corso offre gli strumenti per orientarsi nel Cloud Computing in questo importante momento di transizione e per adottare da subito le "best practices" nella progettazione, realizzazione e gestione delle infrastrutture in ambiente Cloud.

Agenda (1 giorno)

Il Cloud Computing è arrivato e funziona:

- i maggiori fornitori a livello mondiale: Amazon, Rackspace, Google, Softlayer, Windows Azure
- elementi in comune e aspetti unici delle offerte
- case history: gli esempi di eccellenza: Netflix: migliaia di server, NASA: picchi realtime.

Dal Datacenter al Cloud Computing:

- stack per nuvole private: CloudStack, Eucalyptus, OpenStack
- scenari ibridi privato-pubblico
- scenari ibridi pubblico-pubblico
- transizioni fra gli scenari
- case History: Zynga da Datacenter a Public Cloud a Private Cloud specializzata.

Progettare e gestire l'infrastruttura:

- disegno e implementazione: gli approcci Image Bundle e Server Template a confronto
- livelli di astrazione degli elementi di base e servizi specializzati
- gestione e orchestrazione: Chef, Puppet, CloudFlow
- case Study: esempio di architettura 3 tier con Disaster Recovery.

Aspetti economici:

- Cloud Computing: l'IT come utility
- elementi che determinano i costi
- il mercato delle istanze spot
- le istanze riservate e l'aftermarket
- Case History: PlanForCloud.

Obiettivi

Formare nuove competenze in grado di progettare, implementare e gestire un sistema in ambiente Cloud Computing.

Destinatari

Responsabili di sistemi informativi, progettisti.

Prerequisiti

Conoscenza di base su System Administration, Networking.



La gestione documentale

Partendo dai concetti dell'Archivistica "classica" e dagli strumenti metodologici da essa forniti, si affronterà il problema della digitalizzazione dei documenti cartacei, anche tramite esempi di servizi come la Mailroom, per approdare quindi alla gestione elettronica dei documenti. La Conservazione a lungo termine dei documenti in formato elettronico è un problema tutt'ora aperto di cui è importante prendere coscienza, allo scopo di utilizzare fin da subito l'approccio corretto. Si affronterà quindi il tema della sicurezza delle informazioni con particolare enfasi all' ambito elettronico, dove troviamo i concetti di firme digitali, PEC e DRM.

Agenda (3 giorni)

Introduzione all'Archivistica:

- cos'è un documento
- cos'è un Archivio
- il Titolario di classificazione
- il Massimario di scarto
- il Manuale di Gestione
- il Protocollo.
- caratteristiche degli Archivi cartacei.

Lo standard OAIS.

Processi e documenti:

- cos'è il Business Process Management
- ISO 15489.

Dal cartaceo al digitale e ritorno:

- OMR, OCR, ICR, BCR ecc.
- i glifi
- un esempio di servizio: la mailroom.

La conservazione a norma.

Il documento digitale:

- il fascicolo elettronico
- il fascicolo sanitario elettronico
- La fatturazione elettronica.

Sistemi di gestione elettronica dei documenti.

La conservazione a lungo termine dei documenti elettronici.

Introduzione alla sicurezza delle informazioni.

Certificati e firme.

La Posta Elettronica Certificata.

Proprietà intellettuale e Digital Rights Management.

Obiettivi

Fornire un'ampia panoramica sulle tematiche connesse alla gestione documentale, sia cartacea che elettronica.

Destinatari

Responsabili di Sistemi Informativi, manager, consulenti e figure commerciali e di pre-vendita che desiderino dotarsi delle competenze di base necessarie.

Prerequisiti

Nessuno.



La sicurezza dei sistemi, dei dati e delle reti

Il corso affronta il problema della sicurezza, analizzando tutti i componenti a rischio presenti in un'azienda che utilizza reti aperte basate su tecnologia TCP/IP, con particolare attenzione alle vulnerabilità dell'interconnessione con l'Internet pubblica. Una volta introdotte le problematiche di scenario, in relazione agli attacchi ai sistemi e alle possibili azioni e contromisure, vengono presentati approfondimenti specifici sulle tecniche più diffuse tra gli hacker per attaccare un sistema.
L'attenzione viene poi focalizzata sulla crittografia, utilizzata come strumento per assicurare riservatezza e integrità ai dati e per prevenire rischi derivanti dall'accesso non autorizzato alle informazioni veicolate tramite servizi di larga diffusione, come, la posta elettronica e il WWW.
Il corso prosegue analizzando le possibili soluzioni per realizzare una adeguata protezione perimetrale utilizzando i Firewall e per estendere i confini della propria rete privata con l'ausilio di tunnel cifrati tra più sedi e utenti remoti interconnessi tramite una rete dati pubblica.

Agenda (5 giorni)

La sicurezza informatica: lo scenario di riferimento, i concetti base.

Introduzione alla sicurezza aziendale: architettura, gestione e procedure:
- standard di riferimento per la sicurezza: TCSEC, ITSEC, CC.
- una classificazione dei possibili attacchi: esterni/interni
- vulnerabilità intrinseche dell'architettura TCP/IP.

Tecniche per condurre un attacco:
- attacchi di bassa complessità: packet sniffing, spoofing, session hijacking, man-in-the-middle
- anatomia di un attacco e tools usati.

Strumenti per la sicurezza dei dati: crittografia, algoritmi simmetrici e asimmetrici, funzioni di hash:
- algoritmi a chiave simmetrica (DES, AES) e a chiave asimmetrica (DH, RSA)
- applicare la crittografia: firma digitale e certificati digitali.

Esempi applicatici: la sicurezza wi-fi (WEP e WPA).

Problematiche di sicurezza connesse ai principali servizi Internet_based:
- soluzioni per una posta elettronica sicura: PGP e S/MIME
- standard per transazioni commerciali e web: Secure Socket Layer (SSL)
- la sicurezza dei sistemi e delle applicazioni client: es. Internet Explorer e Outlook.

Strumenti di verifica livelli di sicurezza implementati: scanner, IDS:
- strumenti di logging e event correlation.

Le problematiche di sicurezza nell'accesso alle risorse ospitate in una rete aziendale TCP/IP:
- la sicurezza nell'accesso, autenticazione tramite RADIUS server
- la sicurezza nell'accesso tramite Internet pubblica: router, ACL e proxy server
- realizzare una soluzione di sicurezza perimetrale: architetture Firewall, possibili implementazioni.

Estendere i confini della propria rete privata: Reti Private Virtuali (IPSEC).

Obiettivi

Al termine del corso i partecipanti sono in grado di:
- avere una chiara comprensione delle problematiche della sicurezza informatica e delle più comuni tipologie di attacco
- conoscere i principali standard del settore
- padroneggiare gli strumenti più idonei per rivelare/contrastare attacchi informatici.

Destinatari

Responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete, progettisti di sistemi di rete e tutti coloro che desiderano avere una visione d'insieme delle varie tematiche connesse alla sicurezza dei sistemi e delle reti.

Prerequisiti

Conoscenza di base dell'uso delle reti di computer e dei principali protocolli connessi al TCP/IP.



Cyber Security: Minacce e Criteri di Protezione

Il cyberspace è oggi il termine più utilizzato per indicare le dimensioni digitali della società dall'avvento di Internet. Per chi opera a garanzia degli interessi nazionali di un Paese o di una Industria è necessario impostare una propria politica di cyber security che oltre alle tecnologie affronti aspetti sociali, legali ed economici. Le minacce coinvolgono diversi attori. Istituzioni, Industria privata, Cittadini sono vulnerabili e il Cyber Crime può operare acquisendo informazioni riservate e/o delicate da utilizzare per attaccare infrastrutture critiche di vitale importanza o beni tangibili di singoli. Il cyberspace, secondo l'approccio militare, ha la dimensione di un vero campo di battaglia e come tale ci si muove con tecniche di intelligence (Cyber War). Lo scenario internazionale ed italiano si analizza sia in termini legislativi che di processi organizzativi e tecnologici per il contrasto al crimine, unitamente al livello di consapevolezza da parte dei vari settori sia istituzionali che privati di essere obiettivi sensibili e rischiare di poter subire notevoli perdite in termini economici e tecnologici. Gli elementi in gioco sono le infrastrutture critiche, gli asset esposti ai rischi di attacchi cyber in varie tipologie, i danni causati e potenziali, i valori economici in gioco. La cyber security, infatti, non è solo un'esigenza ma anche un'opportunità in termini di capacità industriali e di ricerca.

Agenda (3 giorni)

Quadro di riferimento:

- Cyber Security Standard
- infrastrutture critiche nazionali ed estere identificate, team di difesa e loro differenze (CERT, CSIRT, ecc.)
- report ed evidenze su tipologia, target e danni economici causati dagli attacchi informatici (cyber attacks)
- situazione internazionale in USA, Unione Europea e in Italia anche dal punto di vista normativo
- enti e operatori coinvolti nel governo del Cyber Space e nelle misure di protezione e nelle strategie nazionali
- misure di protezione, di difesa, di resilience e "proattive" per la prevenzione ed il contrasto del Cyber Crime
- indicatori del livello di consapevolezza, difesa, interdipendenza transnazionale e propensione agli investimenti in sicurezza
- analisi delle tecniche di protezione tradizionali ed emergenti e delle minacce correlate (CyberCrime).
-

Obiettivi

Acquisire gli elementi principali sugli aspetti normativi, regolatori, sugli standard di riferimento.
Avere evidenze della situazione internazionale e nazionale in merito dimensione del fenomeno, alle minacce, agli attacchi di tipo Cyber ed ai criteri di protezione.
Analizzare le principali tecniche di attacco e di difesa in funzione del contesto.
Individuare le infrastrutture potenziali obiettivi, le strutture e i centri di prevenzione e di risposta ed il grado di esposizione al rischio degli asset tangibili e non.

Destinatari

Responsabili IT, Security Manager, Forze dell'Ordine e quanti operano nella gestione dei dati informatici e telematici riservati e/o critici per l'erogazione dei servizi o del business.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.



Tecniche di attacco di un sistema informatico

Negli ultimi anni lo sviluppo di strumenti di rilevazione delle vulnerabilità e di attacco sempre più evoluti ed automatizzati – facilmente reperibili in rete – rende possibile che un malintenzionato ("script kiddie"), anche di bassa cultura informatica, acquisisca il controllo di una macchina collegata in rete sfruttandone le vulnerabilità eventualmente presenti. Il corso vuole illustrare la semplicità di diverse tecniche di attacco al fine di comprendere la metodologia usata dagli "hacker" e per poter testare efficacemente, attraverso tecniche di penetration testing, il proprio network, per individuare macchine non configurate correttamente e per comprendere come anche i routers e i firewall, se non configurati correttamente, possano essere violati.

Agenda (3 giorni)



Anatomia di un attacco

- Processo di attacco informatico; Minacce e Vettori di attacco; Raccolta informazioni sul target; Mappatura della rete target; Individuazione delle vulnerabilità di un target; Metodi per violare un target (Password cracking, Installazione agenti ostili su host, recupero e manipolazione informazioni via "Man in the Middle"); Compromissione di un host (preparazione e configurazione di Exploit Code); Trasformazione dell'attacco (apertura di backdoor, cancellazione log).

Raccolta informazioni sul target

- Comprendere le misure di sicurezza adottate dal target; Metodi di raccolta informazioni (diretta e indiretta); Domain name registrati dal target; Indirizzi IP pubblici assegnati al target; Ricostruzione Network Topology; Geolocalizzazione delle sedi che ospitano i sistemi sotto attacco; Sfruttare i Social Network; Utilizzo dei motori di ricerca (Google, SHODAN); Applicazione principi di Social Engineering; Individuazione host ed enumerazione servizi.

Analisi del perimetro e della rete

- Individuazione vie di accesso utilizzabili per raggiungere il target; Enumerazione accessi Internet; Individuazione accessi VPN; War Dialing; War Driving; Riconoscimento di switch, router e firewall; Compromissione di un apparato di rete; Attacchi DOS alla infrastruttura di rete; Iniezione di false informazioni di routing; Modifica delle configurazioni degli apparati; Mapping delle regole di filtraggio dei Firewall; Individuazione di IDS/IPS; Tecniche per bypassare gli strumenti di difesa perimetrale.

Individuazione vulnerabilità su host

- Classificazione delle vulnerabilità; Utilizzare un Port Scanner per la raccolta Banner servizi; Ricerca vulnerabilità del software installato su database pubblici; Strumenti per l'automazione della ricerca di vulnerabilità (Vulnerability Scanner); Vulnerabilità specifiche del Web (XSS, SQL Inijection, CGI); Verifica delle vulnerabilità tramite Penetration Test; Individuazione vulnerabilità.

Password Cracking

- Utilizzo delle password nei meccanismi di autenticazione; Conservazione sicura delle password; Trasmissione delle password via rete; Raccolta password tramite keylogging; Decodifica delle password cifrate; Tecniche per effettuare Password Cracking (brute force, dictionary attack, rainbow table); Test di una password via rete.

Attacchi Man-in-the-middle

- Come ottenere una condizione Man-in-the-middle; Switch Port Mirroring; ARP Poisoning; ICMP Redirection; Policy Routing; Attivazione di un Sniffer di rete; Utilizzo di strumenti di hacking per la manipolazione del traffico intercettato.

Compromissione di un host

- Guadagnare il controllo remoto di un host tramite componenti software già installate; Authentication Bypass; Sfruttamento di bug software per l'iniezione di Malware; Ricerca e configurazione di un Exploit Code; Piattaforme open source di Exploiting (Metasploit); Privilege Escalation; Apertura Backdoors; Cancellazione log.

Obiettivi

Al termine del corso i partecipanti sono in grado di comprendere i tipi di attacco a cui possono essere sottoposti i propri sistemi informatici.

Tecniche di attacco di un sistema informatico

Destinatari

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Conoscenza di base dell'uso delle reti di computer e dei principali protocolli connessi al TCP/IP. È propedeutico il corso SEC302.



Tecniche di difesa di un sistema informatico

Il corso si pone come obiettivo quello di far comprendere le contromisure da adottare per garantire il livello desiderato di sicurezza del proprio sistema informativo. È destinato ai responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; operatori che vogliano acquisire una visione d'insieme delle tematiche connesse alla sicurezza dei sistemi e delle reti.

Agenda (3 giorni)



Valutazione delle misure di sicurezza

- Individuazione degli Asset Informatici; Risk Analysis; Vulnerability Assessment; Penetration Test; Comprendere le minacce che insistono sugli Asset; Requisiti di sicurezza base (riservatezza, integrità, disponibilità); Misure di sicurezza preventive e reattive; Gestione del rischio residuo; Incident Handling.

La sicurezza dei dati

- Ciclo di vita dei dati (produzione, trattamento, conservazione); Proteggere i dati memorizzati; Soluzioni per assicurare la riservatezza e l'integrità dei dati trasmessi; Soluzioni per garantire l'autenticità della sorgente dei dati; Identità digitale; Firma digitale e non ripudio; Autorità di certificazione e certificati digitali; Utilizzo della crittografia nei principali servizi Internet (Web, Mail).

Progettazione di reti sicure

- Suddividere la rete in contesti di sicurezza mutamente separati; Tassonomia soluzioni di accesso alla rete (wired, wireless, LAN, WAN, VPN); La sfida alla sicurezza rappresentata dagli accessi wireless e VPN; Controllo accessi alla rete: EAP e 802.1x; Realizzazione di uno schema AAA tramite RADIUS; Principi di hardening per gli apparati di rete (eliminazione servizi non necessari, protezione tabelle di instradamento e tabelle ARP, blocco protocolli non richiesti); Gestione e controllo degli apparati di rete; Creazione di una rete dedicata al Network Management.

Hardening dei sistemi

- Individuazione delle componenti software necessarie per l'erogazione del servizio; Determinazione della versione del software attivo sul sistema; Mapping tra porte e servizi erogati; Rilevazione vulnerabilità e patch rilasciate dai vendor; Rimozione account di default; Riconfigurazione password amministrative; Eliminazione componenti software non necessarie; Blocco avvio automatico di servizi non indispensabili; Binding tra servizi ed interfacce di rete negli host multihomed; Attivazione funzionalità di logging; Analisi dei log; Conservazione sicura dei log; Installazione Antivirus, Personal Firewall, Host IDS; Integrazione tra controllo accessi alla rete e sicurezza delle postazioni di lavoro tramite Network Admission Control (NAC).

Difendere il perimetro della rete

- Soluzioni di difesa perimetrale; Attivazione di un firewall; Ispezione dei pacchetti a livello applicativo; Blocco della posta indesiderata; Pubblicazione indiretta dei servizi tramite Reverse Proxy; Soluzioni per la rilevazione degli attacchi (IDS); Prevenire la compromissione degli Asset tramite IPS; Raccolta e centralizzazione dei log di sicurezza; Security Information & Event Management.

Obiettivi

Al termine del corso i partecipanti sono in grado di comprendere le contromisure da adottare per garantire il livello desiderato di sicurezza del proprio sistema informativo.

Destinatari

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Conoscenza di base dell'uso delle reti di computer e dei principali protocolli connessi al TCP/IP. È propedeutico il corso SEC302.

Ethical Hacking e Penetration Test di Applicativi Web

Le applicazioni web rappresentano il vettore d'attacco più utilizzato da parte di criminali informatici. I motivi sono molteplici fra cui:

- enorme diffusione
- notevole superficie d'attacco
- scarsa attenzione in fase di progettazione agli aspetti di sicurezza.

Tutto questo ha portato anche alcune grandi realtà come Sony, Yahoo, Apache, ecc. a scontrarsi con fenomeni quali:

- furto di dati riservati e di carte di credito
- *defacement* di siti Web
- spionaggio industriale
- utilizzo di siti web compromessi per diffondere *Malware* e creare *Botnet*
- aumento del "*Ransom Malware*".

Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri applicativi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime. Unire così la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta ormai una necessità irrinunciabile. Saranno affrontate anche tematiche di "raccolta delle informazioni" ("Information Gathering") e tecniche e tools di cracking di password e hash. Sono previste, molte esercitazioni tratte da casi reali.

Agenda (3 giorni)



Associazioni, risorse e documentazione sulla sicurezza delle applicazioni web.

Metodologia ed analisi di tipo "Black-Box"/"White Box".

"Modus Operandi" e l'importanza del pensiero "out-of-the-box".

La distribuzione Linux BackTrack: concetti di base, architettura generale e panoramica dei principali tools installati.

Altre distribuzioni Linux utili al Security Assessment di applicativi web.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Password/Hash Cracking.

Vulnerabilità delle applicazioni web, evasione di WAF e contromisure.

Laboratorio ("Capture The Flag!").

Indicazioni per la scrittura di un report finale di Penetration Test applicativo.

Obiettivi

Illustrare le principali e più diffuse vulnerabilità delle applicazioni web, nonché i più comuni errori nella scrittura di un applicativo web dal punto di vista della sicurezza.
Analizzare gli attuali attacchi client-side e server-side.

Destinatari

Personale che si occupa della verifica della sicurezza di applicativi e sistemi, IT Security Engineer, sviluppatori di applicativi, responsabili della sicurezza IT.

Prerequisiti

Conoscenze di base dei concetti relativi al funzionamento di applicativi e sistemi e di rete. Conoscenze di base delle principali problematiche della IT security.



Ethical Hacking e Penetration Test: dalla teoria alla pratica

La sicurezza informatica non può risolversi solo nella progettazione ed ingegnerizzazione di un'architettura di rete ed applicativa, basata sul principio meglio conosciuto come "Sicurezza Difensiva". Questo modo di procedere rappresenta una forte limitazione, producendo a volte danni economici e d'immagine, quali:

- furto di carte di credito
- furto di dati riservati
- violazione di sistemi web, scada, rete, ecc.
- spionaggio industriale, governativo o militare
- "Malware Banking"
- "Ransom Malware".
- che non hanno risparmiato grandi realtà come Sony, Yahoo,...
- Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri sistemi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime.
- Unire la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta una necessità irrinunciabile.

Agenda (5 giorni)



Associazioni, risorse e documentazione utili ad un Penetration Tester.

Metodologia ed analisi di tipo "Black-Box"/"White Box".

"Modus Operandi" e l'importanza del pensiero "out-of-the-box".

La distribuzione Linux BackTrack: concetti di base, architettura generale e panoramica dei principali tools installati.

Altre distribuzioni Linux utili ad un Penetration Tester.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Attacchi di reti di tipo *M.I.T.M.*

Buffer Overflow.

Vulnerabilità delle applicazioni web.

Password / Hash Cracking.

V.A., Exploitation e Post-Exploitation.

Cenni al funzionamento ed evasione di programmi Antivirus.

Indicazioni per la scrittura di un report finale di un Penetration Test.

Obiettivi

Alla fine del corso i partecipanti acquisiscono tecniche e metodologie utilizzate durante una attività di Penetration Test di applicativi, rete e sistemi e sono in grado di realizzare in autonomia i Penetration Test.

Destinatari

Personale che si occupa della verifica della sicurezza di applicativi e sistemi, IT Security Engineer, responsabili della sicurezza IT.

Prerequisiti

Conoscenze di base dei concetti relativi al funzionamento di applicativi e sistemi e di rete. Conoscenze di base delle principali problematiche della IT security.



Sicurezza di rete: firewall, IPS e VPN

Uno dei problemi più importanti nei sistemi informativi aziendali è la protezione del proprio sito da attacchi esterni provenienti da Internet. Le prime azioni di difesa sono affidate ai "Firewall", che controllando i punti di accesso minimizzano il rischio di accessi non autorizzati. Per integrare le funzionalità del Firewall e soprattutto per ridurre il rischio di attacchi provenienti dall'interno si può aggiungere il controllo eseguito dagli IDS/IPS, che esaminano il traffico alla ricerca di azioni illecite e/o di codice malevolo.
Il corso si conclude con l'esame delle diverse soluzioni di reti private virtuali che, utilizzando una infrastruttura pubblica, permettono di interconnettere i siti su base geografica.
Il corso offre una visione d'insieme delle tematiche connesse alla sicurezza dei sistemi e delle reti.

Agenda (4 giorni)

La sicurezza in Internet/Intranet: analisi dei principali requisiti di sicurezza e delle minacce delle reti TCP/IP.

Tecnologie di firewalling e meccanismi di funzionamento:

- descrizione delle funzionalità di base di un firewall
- progettazione della politica di sicurezza di un firewall
- tipologie di firewall (Packet filter, Application proxy, stateful) e loro campi di impiego.

Funzionalità accessorie di un firewall:

- Network Address Translation (NAT), Port Address Translation (PAT)
- Virtual Private Network (VPN)
- High availability, load balancing.

Selezione di prodotti di firewalling:

- Rassegna dei principali prodotti di firewalling commerciali
- Rassegna dei principali prodotti in libera distribuzione
- Linee guida sulla selezione di un prodotto di firewalling.

Architetture implementative di firewalling:

- modelli architetturali per la protezione di una Intranet da reti esterne interconnesse (Internet, altri Sistemi informativi)
- modelli architetturali per la realizzazione di aree protette all'interno della Intranet
- architetture per l'alta affidabilità/load balancing.

Intrusion prevention system:

- IDS ed IPS
- descrivere come i sensori possono limitare gli attacchi
- conoscere i parametri di sistema essenziali
- analizzare gli eventi e sintonizzare un sensore.

Reti private Virtuali (VPN):

- protocollo IPSec, tunnel e transport mode, main e aggressive mode.

Obiettivi

Al termine del corso i partecipanti sono in grado di comprendere e saper utilizzare gli apparati di rete per garantire il livello di sicurezza richiesto.

Destinatari

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Buona conoscenza della suite di protocolli TCP/IP.



OpenVPN e CISCO VPN

Il corso affronta le tematiche della sicurezza di rete, in particolare, le diverse soluzioni di infrastrutture VPN (Virtual Private Networks) basate su sistemi Unix-like e/o interoperabili con apparati CISCO.

Agenda (4 giorni)



Panoramica sulle soluzioni VPN disponibili su Linux.

IPSEC: Principi e protocollo.

IPSEC: Installazione e configurazione su apparati CISCO in Alta Disponibilità.

IPSEC: Interoperabilità con sistemi e apparati terzi (es. Microsoft).

IPSEC: VPN Lan2Lan.

OPENVPN: Installazione e configurazione anche in Clustering/Virtualizzazione.

OPENVPN: Interoperabilità con Windows.

SSH: Tunnel e port forwarding.

Soluzioni di port knocking

Obiettivi

Al termine del corso i partecipanti sono in grado di saper installare e configurare una VPN basata su OpenVPN, saper installare e configurare una VPN su router CISCO, conoscere le potenzialità di tunneling e portforwarding di SSH, valutare soluzioni di port knocking.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco, sicurezza delle reti e gestione sistemistica di sistemi Unix-like.



Reti sicure in ambiente SonicWall, aspetti di base

Il corso garantire ai discenti di acquisire le conoscenze necessarie per poter mettere in esercizio e configurare firewall SonicWall. Ciò comporta la capacità di gestire le operazioni quotidiane dei dispositivi SonicWall a supporto di specifiche politiche aziendali. Questo corso, dopo la presentazione della famiglia di prodotti SonicWall, ha l'obiettivo di fornire una solida comprensione della configurazione e del monitoraggio quotidiano dei dispositivi SonicWall.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione SonicWall Network Security Basic Administration (NS-102-A).

Agenda (2 giorni)





Registrazione del prodotto.

System Backup & Restore.

WAN ISP Failover and Load Balancing.

Policy Based Routing.

VPN: Gateway-to-Gateway, Hub and Spoke, Mesh.

GVC with Local User DB.

SSL VPN & Global VPN Client with LDAP Authentication.

Content Filtering Service using Single Sign-On.

Security Services.

Troubleshooting.

Appendix: High Availability.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dagli apparati SonicWall.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione SonicWall Network Security Basic Administration (NS-102-A).

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.

Reti sicure in ambiente Cisco, difesa perimetrale con IOS Firewall

Il corso presenta le varie tipologie di attacco a cui può essere sottoposta una rete enterprise e le tecniche atte a mitigare tali attacchi attivando le funzionalità di sicurezza che sono presente nei sistemi operativi dei router e degli switch: controllo degli accessi, firewall ed IPS. Inoltre, essendo le reti enterprise geografiche sempre più spesso realizzate utilizzando backbone IP, il corso illustra come mettere in sicurezza le reti usando le reti private virtuali.
Per ciascuna soluzione vengono valutati gli aspetti di sicurezza e le metodologie pratiche di messa in sicurezza degli apparati costituenti la rete, con particolare riferimento agli apparati Cisco. Il corso prevede, oltre alla descrizione teorica degli argomenti trattati, una rilevante attività di laboratorio 'hands on' su un ricco laboratorio, costituito da router e switch Cisco, nel quale sono riprodotte situazioni analoghe a quelle reali. Oltre alle operazioni di configurazione saranno effettuate esercitazioni che, partendo da reti già configurate, mirano ad aggiungere servizi/applicazioni ed a modificare le configurazioni dei dispositivi per conseguire miglioramenti nella sicurezza della rete.

Agenda (5 giorni)





Sicurezza a livello di data link:

- tipi di attacchi
- come mitigare gli attacchi
- mettere in sicurezza il layer 2: PVLAN, controllo del DHCP e dell'ARP.

Gestione degli accessi alla rete: 802.1X.

Network Foundation Protection: mettere in sicurezza il piano dati, gestione e controllo.

Dispositivi di Sicurezza nei router Cisco:

- Network address translation
- Cisco IOS Firewall
- implementazione e configurazione di Cisco IOS firewall in modo classico (interface-based)
- implementazione e configurazione di Cisco IOS firewall basato sulle zone (zoned-based)
- configurare l'Authentication Proxy
- Cisco IOS IPS
- implementazione e configurazione di Cisco IOS IPS.

Reti Private Virtuali:

- il protocollo IPSec
- implementazione di VPN IPSec con pre-shared keys e con PKI
- implementazione di VPN IPSec facilmente scalabili
- configurazione di Tunnel GRE su IPSec
- configurazione di VPN su più siti, Dynamic Multipoint VPN
- configurare VPN altamente affidabili
- implementare l'accesso remoto
- configurazione di VPN SSL
- configurazione di Easy VPN.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza – firewall, IPS e VPN – messi a disposizione dal l'IOS dei router e degli switch.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.



PCI DSS v2.0 (Payment Card Industry Data Security Standard)

Lo standard PCI DSS ha lo scopo di migliorare la sicurezza dei dati relativi ai pagamenti, riducendo le frodi nelle operazioni con carta di credito. Il corso illustra i 13 “Requirements” e più di 220 sub-requirements che compongono lo standard.
La v1.2 –rilasciata il 1 ottobre 2008 specificava sei gruppi, definiti obiettivi di controllo, in cui venivano inseriti i requirements. L’attuale versione v2.0 in vigore dal 1 gennaio 2011 rivede il ciclo di vita dello standard, comprende l'inserimento dei componenti virtuali di sistema, chiarisce le relazioni con la PA DSS, approfondisce lo sviluppo software e rivede il ranking delle vulnerabilità oltre ad inserire un nuovo tipo C-VT.

Agenda (2 giorni)

Introduzione alle problematiche di sicurezza delle transazione con carta di credito.

Introduzione agli standard PCI.

Analisi degli obiettivi di controllo del PCI DSS:

- costruire e mantenere la rete sicura
- proteggere i dati di titolari di carta
- utilizzare programmi per la gestione delle vulnerabilità
- implementazione di rigide misure di controllo dell’accesso
- monitorare e eseguire test sulle reti regolarmente
- definire una politica di sicurezza delle informazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze di tutti i requirements dello standard PCI DSS.

Destinatari

Responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Nessuno.

Reti sicure in ambiente Cisco, difesa perimetrale e accesso remoto con ASA NG

Il corso affronta come le tematiche della sicurezza perimetrale e dell'accesso remoto possono essere risolte usando in rete apparati Cisco ASA Next Generation configurati opportunamente. In particolare è illustrato come configurare e implementare le policy che i nuovi apparati Cisco ASA Next Generation devono imporre nei punti perimetrali esterni ed interni. Gli argomenti su cui verteranno le lezioni sono principalmente le tecnologie utilizzate per rafforzare la sicurezza del perimetro di una rete: Network Address Translation, Intrusion Prevention System, policy e application inspect. Il corso affronta successivamente le soluzioni Virtual Private Network (VPN) che gli ASA mettono a disposizione: IPsec-VPN, SSL VPN, anyconnect, IPsec VTI, DMVPN, FlexVPN.

Agenda (5 giorni)





Principi di sicurezza perimetrale:

- Zone di Sicurezza, Architetture modulari, SecureX, TrustSec.
- Funzionalità di un Firewall:
  - Stateless Packet Filtering
  - Application Layer Gateway (Proxy)
  - Stateful Packet Filtering (SPF)
  - Application Inspection and Control Filtering (AIC)
  - Context-Aware Firewalls
- Funzionalità complementari

Sviluppo di protezione dell'infrastrutture di Rete:

- Sicurezza sul control plane Cisco IOS
- Sicurezza sul Management plane Cisco ASA

NAT su Cisco IOS e ASA:

- Configurare il NAT (Network Address Traslation) sugli ASA
- Configurare network object, static NAT usando network object NAT, dynamic PAT usando netvork object NAT
- Configurare twice NAT o manual NAT
- Configurare dynamic NAT usando manual NAT
- Configurare twice NAT usando manual NAT

Controlli delle minacce sul Cisco ASA:

- Implementare policy base su Cisco ASA
- Implementare policy avanzate su Cisco ASA
- Implementare policy Reputation-based su Cisco ASA
- Implementare policy Identity-based su Cisco ASA.

Cisco ASA Next-Generation Firewall (NGFW):

- Cisco ASA NGFW
- Architettura Cisco ASA NGFW
- Implementare Policy Objects su ASA NGFW
- Monitoring del Cisco ASA NGFW
- Implementare access policies su Cisco ASA NGFW
- Implementare identity policies su Cisco ASA NGFW
- Implementare decryption policies su Cisco ASA NGFW.

Cisco Intrusion Prevention System:

- Configurazione base del Cisco IPS
- Tuning del Cisco IPS
- Configurazioni personalizzate delle signaures IPS
- Configurare le Anomaly Detection nel Cisco IPS
- Configurare le Cisco IPS Reputation-Based.

Fondamenti di crittografia e Tecnologia VPN:

- Il ruolo delle VPN nella sicurezza della rete
- VPN e crittografia.

Implementare IPsec point-to-point su Cisco ASA:

- Soluzioni Cisco Secure site-to-site
- Implementare VPN IPsec point-to-point con Cisco IOS FlexVPN
- Implementare VPN IPsec Hub-and-spoke con Cisco IOS FlexVPN.

Implementare clientless SSL VPNs:

- Implementare Clientless SSL VPNs
- Implementare Clientless SSL VPNs su Cisco ASA
- Implementare applicazioni di accesso per clientless su Cisco ASA
- Implementare Authentication and Authorization avanzata per clientless VPN SSL
- Implementare policy Identity-based su Cisco ASA.

Implementare Cisco AnyConnect VPN:

- Implementare AnyConnect SSL VPN base su Cisco ASA
- Implementare AnyConnect SSL VPN azanzato su Cisco ASA
- Implementare Authentication e Authorization su Cisco AnyConnect VPN
- Implementare Cisco VPN AnyConnect IPSec/IKEv2.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

- identificare le caratteristiche dei modelli di Security Appliance in commercio
- configurare il Firewall dalla command line interface e graficamente attraverso l'ASDM
- realizzare VPN con implementazione della AAA
- abilitare un accesso protetto di gestione da remoto dei Security Appliance.

Destinatari

Responsabili di sistemi informativi di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; sistemisti di rete; supervisori di sistemi di sicurezza.

Prerequisiti

Buona conoscenza dell'architettura TCP/IP e dell'Internetworking IP in ambiente Cisco.



La sicurezza nei Sistemi operativi Windows: aspetti e strumenti di gestione

Il corso illustra gli aspetti di sicurezza di Windows sia lato server che lato desktop. Per Windows Server 2008/2012 si esamina, innanzitutto, la configurazione di Active Directory, proseguendo con l'utilizzo dei Group Policy, per terminare con l'analisi degli aspetti di sicurezza a livello di rete, software, file e cartelle. Per Windows 7/8, invece, si analizzano gli aspetti di sicurezza locale, di rete ed internet. Infine viene descritta la configurazione ottimale di Internet Explorer.

Agenda (5 giorni)

Sicurezza in Windows Server 2008/2012

Ruoli di Windows Server.

Active Directory Domain Services:

- creazione di account di utenti e computer
- creazione di gruppi e unità organizzative
- amministrare l'accesso alle risorse
- amministrare AD DS Trusts.

Creazione e configurazione di Group Policy.

Configurare utenti e computer utilizzando Group Policy.

Amministrare la sicurezza del server tramite WSUS e Audit policy.

Implementare IT Security Layers.

Implementare la sicurezza di file e cartelle.

Implementare la sicurezza di rete.

Implementare la sicurezza del software.

Sicurezza in Windows 7/8

Configurare i profili utente.

Windows Workgroups e Active Directory Domains.

Condivisione delle cartelle.

Utilizzare NTFS Encryption.

Connettere Windows 7/8 in rete.

Implementare la sicurezza locale, di rete ed internet.

Configurare Internet Explorer.

Obiettivi

Fornire le competenze per rendere sicuri i sistemi operativi Windows Server 2008/2012 e Windows 7/8.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenze di networking di base e dei sistemi operativi Windows Server 2008/2012, Windows 7/8.

Progettare e realizzare la sicurezza di Sistemi Operativi Microsoft Windows

Il rischio di vulnerabilità di sistemi Windows può essere notevolmente ridotto con una opportuna configurazione del sistema. Mentre alcuni accorgimenti dovrebbero essere presi in ogni situazione, la configurazione più adatta a mettere in sicurezza un sistema in ogni contesto di esercizio deve essere valutata di caso in caso. Per raggiungere questo livello di abilità, è necessario conoscere in dettaglio il progetto e l'implementazione della sicurezza di sistemi basati su piattaforme Windows Server e Client.

Agenda (5 giorni)

Funzionalità e strumenti di sicurezza base dei sistemi operativi Windows.

Richiami sul modello di sicurezza nei sistemi Windows:

- gestione delle utenze, dell'autenticazione, dell'autorizzazione, Access Control List
- sicurezza del file system, dei processi, del sottosistema I/O, del sistema di memory management.

Tecniche tradizionali di intrusione nel sistema:

- cracking delle password ed impersonamento; Virus e minacce correlate; Memory leak e Buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Windows:

- implementazione e configurazione del TCP/IP e del Netbios Windows
- servizi di rete base del S.O. (RPC; Servizi di naming: NetBios e DNS; File Sharing, Distributed File Sharing e Print Sharing; Web Server: IIS; Remote Control di sistemi Windows)
- gestione distribuita delle utenze (Domain Controller, Active Directory) e configurazioni avanzate del sistema di autenticazione e autorizzazione
- rilevazione delle intrusioni tramite logging e auditing
- l'event viewer di Windows
- tecniche di rilevazione statistica delle intrusioni: strumenti di monitoraggio statistico e real time del sistema
- software di intrusion detection
- tecniche di rilevazione basate su regole: utilizzo di firewall locali.

Hardening e Policy Compliance: Windows Domain e Group Policy; Network Access Protection.

Protezione dei dati e delle comunicazioni:

- utenti mobili e BIT Locker
- cifrare le comunicazioni con i certificati
- Remote Access in SSL VPN
- Windows Direct Access.

Soluzioni e architetture di prodotti anti virus: trade-off nelle prestazioni di sistemi protetti da sistemi antivirus.

Dimostrazioni e esercitazioni.

Analisi della configurazione di prodotti: per la difesa/attacco di un sistema: Sniffer, Spoofer, Portscanner per l'hardening di un sistema operativo in libera distribuzione: software di firewalling per la cifratura e la firma di posta elettronica: configurazione ed uso di certificati digitali con Netscape, MS-Explorer, MS-Outlook.

Obiettivi

Al termine del corso i partecipanti hanno conoscenze in dettaglio e competenze per configurare e gestire la sicurezza dei sistemi operativi Windows, sia stand alone che nelle più complesse configurazioni in rete.

Destinatari

Responsabili di S.I., CED e di infrastrutture di rete, Progettisti e amministratori di sistemi di rete, Consulenti junior di Security management, Sistemisti di rete, Supervisori di sistemi di sicurezza.

Prerequisiti

Buona conoscenza dei sistemi operativi Windows, delle reti di computer, della suite di protocolli TCP/IP e conoscenza di base sulla amministrazione di sistemi informativi complessi.



La sicurezza nei Sistemi operativi UNIX/Linux

I rischi di vulnerabilità di sistemi Unix può essere notevolmente ridotto con una opportuna configurazione del sistema stesso. Mentre alcuni accorgimenti dovrebbero essere presi in ogni situazione, la configurazione più adatta a mettere in sicurezza un sistema in ogni contesto di esercizio deve essere valutata di caso in caso. Per raggiungere questo livello di abilità, è necessario conoscere in dettaglio il progetto e l'implementazione della sicurezza di sistemi basati su piattaforme Unix.

Agenda (4 giorni)



Funzionalità e strumenti di sicurezza base dei sistemi operativi Unix/Linux.

Richiami sul modello di sicurezza nei sistemi Unix/Linux:

- gestione di: utenze, autenticazione, autorizzazione; Access Control List
- sicurezza di: file system, processi, sottosistema I/O e sistema di memory management.

Tecniche di intrusione nel sistema:

- cracking delle password ed impersonamento
- memory leak
- buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Unix/Linux.

Personalizzazioni del kernel per attuare le contromisure.

Implementazione e configurazione del TCP/IP.

Servizi di rete base del S.O.:

- servizi di identificazione; SMTP; File Sharing; Web Server; esportazione del display
- gestione distribuita delle utenze: NIS/NIS+. YP
- gestione delle utenze delle applicazioni di rete: mail, web.

Rilevazione delle intrusioni tramite logging e auditing:

- standard syslog
- tecniche di rilevazione statistica delle intrusioni:strumenti di monitoraggio statistico e real time
- software di intrusion detection
- tecniche di rilevazione e filtraggio basate su regole (Linux):Ipchain/Iptables.

Esercitazioni:

- analisi della configurazione di prodotti per la difesa/attacco di un sistema:Sniffer, Spoofer, Portscanner
- analisi della configurazione di prodotti per l'hardening di un sistema operativo
- strumenti per la verifica della tenuta di Firewall e strumenti IDS.

Analisi della configurazione di prodotti per la implementazione di SSL ed HTTPS:

- configurazione di un client e di un server.

Obiettivi

Il corso è finalizzato ad acquisire le competenze per la configurazione e gestione della sicurezza dei S.O. Unix/Linux, sia stand alone sia nelle più complesse configurazioni in rete.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base di S.O., reti di computer, suite di protocolli TCP/IP e della amministrazione di sistemi informativi complessi.

 

Application Security:
criteri e aspetti operativi per lo sviluppo di applicazioni sicure

Lo sviluppo di applicativi sicuri è il passo principale per contrastare le minacce e le vulnerabilità che potrebbero essere insite nelle applicazioni web. Con la progressiva diffusione di architetture distribuite, aperte e flessibili, garantire la sicurezza e l'integrità dei sistemi informativi aziendali è divenuto un compito complesso; se da un lato le applicazioni web hanno portato evidenti benefici in termini di fruibilità per l'utente, dall'altro hanno sicuramente introdotto un nuovo elemento debole ai sistemi. Il requisito della sicurezza nelle applicazioni web che diventa, ad oggi, uno dei principali problemi che affligge questa tecnologia. L'Open Web Application Security Project (OWASP) è un'organizzazione mondiale no profit, che si pone come obiettivo il miglioramento continuo della sicurezza delle applicazioni software, evidenziando sfide e criticità, in modo da permettere a imprese e organizzazioni di prendere decisioni efficaci e adottare soluzioni concrete per contrastarne i rischi.

Agenda (3 giorni)

Scenari e mandatory principles in materia di sicurezza applicativa.

Criteri e metodologie da adottare per lo sviluppo di applicazioni sicure.

Normativa in materia di sviluppo di codice sicuro, introduzione all'OWASP e alle politiche correlate.

Principi fondamentali di testing.

Test di applicativi web, reporting, casi ed esempi.

Ambiti e Perimetri interessati:

- ciclo di vita del software
- ambienti di sviluppo, collaudo ed esercizio di applicazioni
- analisi dei principali tool di mercato e open source
- descrizione della documentazione necessaria e di come condurre le verifiche.

Obiettivi

Acquisire le competenze di base per la scrittura di applicazioni sicure.
Acquisire i criteri per condurre un progetto di Secure Code.
Acquisire le conoscenze in merito alle metodologie e ai principali tool per la scrittura e la verifica di codice sicuro da adottare anche ai fini di conformità richieste.
Individuare i requisiti richiesti per la scelta di piattaforme e tool idonei al proprio contesto aziendale.

Destinatari

Responsabili IT, IT Administrator, Project Manager, Analisti, Programmatori e quanti operano negli ambienti di disegno e sviluppo software, di collaudo e di esercizio di applicazioni informatiche e di porting da ambienti legacy al web.

Prerequisiti

Conoscenze di base di informatica e fondamenti di sviluppo di applicazioni web.



Autorità di certificazione, certificati digitali, carta nazionale dei servizi e posta elettronica certificata

Le tecnologie utilizzate per la sicurezza fondate sul principio delle chiavi asimmetriche sono state utilizzate in unione a precise normative europee e, di conseguenza, italiane allo scopo di realizzare degli strumenti finalizzati all'uso di servizi per i cittadini, partendo dalle categorie professionali e proseguendo con la cittadinanza "informaticamente evoluta", utilizzatrice abitudinaria di risorse internet. Questo scenario ha introdotto necessariamente delle problematiche di carattere normativo prima e di interoperabilità tecnologica poi. Infatti, sempre più frequentemente i "system manager" e più in generale gli addetti informatici specializzati nell'help desk sia a livello operativo, che a livello di responsabilità, hanno a che fare con questa situazione ibrida che rende gli strumenti informatici "legalmente validi", obbligandoli a confrontarsi con uno scenario molto diverso da quello presidiato esclusivamente per via tecnica.

Agenda (3 giorni)

Autorità di certificazione:

- Requisiti di una Autorità di certificazione; Procedura di accreditamento; Procedure operative; Infrastrutture tecniche; Infrastrutture fisiche e continuità operativa; Circuito di emissione; Ciclo di vita dei certificati; Sistemi di pubblicazione dello stato dei certificati.

Firma digitale:

- Direttiva europea sulle firme elettroniche; Quadro normativo italiano attuale; Diffusione della firma digitale; Standard di riferimento per le smart card; Come funzione la firma digitale; Struttura dei certificati; Componenti di un kit di firma digitale; Quadro normativo attuale; Formati della firma digitale: PKCS#7, PDF, XML; Firma digitale singola e firma digitale automatica; Procedure di verifica della firma digitale; Integrazione della firma digitale nei processi informatici tipici del "e-government"; Marcatura temporale.

Posta elettronica certificata (PEC):

- Quadro normativo attuale; Cosa è e a cosa serve; Quadro normativo attuale; Funzionamento del servizio; Standard tecnologici; I gestori di PEC; Attivazione del servizio; Interoperabilità con servizi di posta "standard"; Ambiti di applicazione.

Carta Nazionale dei Servizi (CNS):

- Quadro normativo attuale; Regolamento concernente la diffusione della CNS; Standard di riferimento per le smart card; Struttura dei certificati di autenticazione; Descrizione della tecnologia e costituzione di una CNS; Circuito di emissione; Utilizzo di una CNS: autenticazione, firma digitale, pagamenti; Interoperabilità; Applicazioni in ambito sanitario della CNS; Architetture di sicurezza.

Obiettivi

Offrire un'adeguata e aggiornata formazione orientata a comprendere le funzioni, le norme e relative implicazioni e i requisiti di sistema delle tecnologie informatiche asservite alla digitalizzazione della pubblica amministrazione.

Destinatari

Responsabili di sistemi informativi, Responsabili di progetti IT, tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base delle infrastrutture PKI, dell'uso delle reti di computer, dei principali protocolli connessi al TCP/IP. Conoscenza di base del significato del rispetto dei livelli di servizio e processi di comunicazione B2B, B2G e B2U.



Rilevamento della sicurezza di un sistema informatico

Le pubbliche amministrazioni a seguito dell'introduzione del Codice per l'Amministrazione Digitale (CAD) nel 2006, e successive modificazioni, hanno avviato una profonda attività di ristrutturazione dei processi con particolare riguardo alla trasformazione in digitale dei processi cartacei. In questo processo, gli aspetti formativi sono fondamentali, come sottolineato dalla DigitPA.
Il rischio è infatti l'inefficienza del Personale perché non formato alle nuove tecnologie di trattamento digitale delle informazioni. La logica dei bit è molto diversa da quella della carta; pertanto sono necessari percorsi formativi che portino ad un'innovazione non traumatica dei processi.

Agenda (3 giorni)

Schemi di riferimento della sicurezza nei processi.

Audit interno, Azioni correttive, Azioni preventive.

Controllo gestionale, Sicurezza del personale, Sicurezza fisica.

Manutenzione e sviluppo dei sistemi (SDLC)

Continuità operativa.

Rispetto di leggi vigenti, norme specifiche.

Classificazione degli attacchi, Tecniche e Strumenti.

Schemi metodologici per i test di sicurezza.

L'utilizzo di NESSUS.

Conduzione e predisposizione dei test, analisi dei risultati, presentazione dei risultati e attività di revisione.

Aree di operazione: fisica, logica ed organizzativa.

Aspetti generali di una certificazione, Schemi di certificazione.

Nozioni sulle certificazioni ISO 27001, ISO 27002.

Analisi dei rischi.

Piano gestione rischi.

Requisiti di un sistema di gestione della sicurezza

Limitazioni della responsabilità nella esecuzione delle operazioni.

Piano di rientro, Supporto all'applicazione del piano di rientro.

Esercitazione pratica sulla redazione di un piano di verifica di vulnerabilità.

Esame di risultati relativi a test già condotti.

Strumenti software open source.

Incidenti informatici e Analisi forense – cenni.

Obiettivi

Al termine del corso i partecipanti hanno acquisito la conoscenza:
- sui costituenti reali che sono coinvolti in un sistema informativo complesso, esaminato come risultante di una interazione tra gli elementi fisici, logici ed organizzativi di una organizzazione pubblica e/o privata
- di base su metodologie di processo di sicurezza certificato e norme correlate.

Destinatari

Manager IT, Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza.

Prerequisiti

Conoscenza di base delle reti di computer, dei principali protocolli di internet e delle norme base per il trattamento dei documenti elettronici.



ICT Security: aspetti di base

Il personale interno di ogni organizzazione deve essere consapevole dei rischi legati all'attività che svolge quotidianamente utilizzando il computer aziendale. Solo così è possibile prevenire, almeno in parte, incidenti e minacce alla sicurezza informatica dell'azienda stessa.
Il corso mira a far conoscere i rischi in ambito IT e offre una panoramica sulle attività di prevenzione e sugli strumenti (open e commerciali) da utilizzare per migliorare la sicurezza delle informazioni in azienda.

Agenda (3 giorni)

ICT security overview.

External attack.

Internal attack.

Analisi delle vulnerabilità tecniche.

Out of the box – the hacker's mind.

Il social engineering.

Gestione degli accessi.

Policy e procedure.

Wireless security.

Gestione degli incidenti.

Sistemi di gestione per la sicurezza delle informazioni.

Certificati digitali, firma digitale e Posta elettronica certificata.

Aspetti legali.

Principi di crittografia.

Cenni di computer forensic.

Esercitazioni pratiche.

Obiettivi

Acquisire la conoscenza sui principali aspetti della sicurezza ICT e sulle attività aziendali in termini di prevenzione ed utilizzo dei sistemi in dotazione al personale.

Destinatari

Manager di sistemi informativi, supervisori di sistemi di sicurezza e quanti debbano conoscere le buone pratiche sul tema.

Prerequisiti

Conoscenza dei principali strumenti ICT.



Gestione degli incidenti in un sistema informativo (Incident Management)

I danni causati dalle intrusioni ai sistemi informativi sono direttamente proporzionali alla criticità delle informazioni contenute. Le attività di gestione dell'incidente, qualora si rilevi una violazione, attraverso un Team pronto ad intervenire in tempi brevissimi, sono finalizzate a:

- ricostruire l'evento e isolarne le cause
- comprendere il grado di compromissione delle risorse
- limitare l'entità dei danni subiti e neutralizzare la minaccia
- prevenire nuove violazioni
- raccogliere/predisporre le informazioni sull'incidente per eventuali indagini giudiziarie.

Agenda (3 giorni)



Eventi ed incidenti.

Realizzazione di policy operative, piani, procedure e liste di controllo per la risposta ad incidenti.

Struttura del Team di risposta agli incidenti.

Operazioni gestite dal Team.

Gestire un incidente.

Rilevamento ed analisi.

Contenimento, eliminazione e recupero.

Attività a seguito dell'incidente.

Gestire diverse tipologie di incidente

Normative di riferimento.

Evidenza informatica.

Mezzi di ricerca della prova.

Modalità di intervento.

Acquisizione dell'evidenza informatica.

Computer forensic.

Strumenti software open source per la implementazione della piattaforma di test.

Obiettivi

Acquisire la conoscenza sulle linee guida per la definizione di un piano per la gestione degli incidenti: definizione delle policy, costituzione del Team, predisposizione dei dispositivi hardware e software. Sono tenute in considerazione le norme vigenti e le modalità di ricerca ed analisi delle evidenze informatiche.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza delle reti di computer e dei principali protocolli di Internet. Conoscenza delle norme base per il trattamento dei documenti elettronici.



La Gestione della Continuità Operativa - Business Continuity Management

L'obiettivo primario della Gestione della Continuità Operativa è consentire all'azienda di proseguire le proprie attività anche in condizioni estreme, adottando opportune strategie di continuità, di ripristino e di gestione della crisi al fine di salvaguardare la propria immagine, gli interessi dei clienti e la propria capacità di creare valore.
Da un semplice approccio tecnologico, dopo l'attentato dell'11 settembre, la Gestione della Continuità Operativa ha rivolto l'attenzione non solo agli aspetti di ripristino dei sistemi ma anche a quella che oggi è definita la *social security*.
L'obiettivo primario del corso è fornire ai partecipanti tutte le informazioni, teoriche e pratiche, per comprendere e progettare un piano di continuità operativa in accordo con le strategie aziendali al fine di rendere l'azienda più resiliente a potenziali minacce e ripristinare l'operatività nei tempi stabiliti.
Il corso inoltre tratta aspetti di contorno come i test dei piani e le strategia di comunicazione durante una crisi.

Agenda (3 giorni)



La Continuità Operativa: introduzione e obiettivi.

Best practice di settore.

ISO 22301:2012 – Business Continuity Management System.

Concetti di social security.

Il Disaster Recovery Insitute™ (DRI).

Le Professional Practice DRI™.

Piani di continuità operativa.

Emergency Response.

Piani di Disaster Recovery.

Scelta della Strategia di Recovery.

Legislazione in materia di continuità operativa (PA e privati).

La business Impact Analysis (BIA).

Legami tra continuità operativa e analisi dei rischi.

Legami tra continuità operativa e BIA.

Test dei piani di continuità operativa.

Crisis Communication.

Obiettivi

Al termine del corso i partecipanti hanno acquisito la conoscenza su:

- contenuti di un piano di Business Continuity
- modalità di scelta e realizzazione di un piano di Disaster Rcovery
- best practice di settore (DRI, ISO, ISACA).

Destinatari

Manager IT, Responsabili della sicurezza informatica, Responsabili di area, operatori IT.

Prerequisiti

Conoscenza di base della Information Technology e degli aspetti basilari relativi alla sicurezza delle informazioni.



Analisi dei Rischi informatici

Il corso si basa prevalentemente su esercitazioni pratiche, che permettono al discente di avere una conoscenza dell'argomento sul campo, attuando immediatamente, sotto la supervisione del docente, quanto appreso teoreticamente.
Il corso si basa sulla metodologia MAGERIT e sul tool EAR-PILAR, ma fornisce anche le basi per operare con qualunque altra metodologia.

Agenda (3 giorni)



Elementi base del concetto di rischio.

Metodologie qualitative e metodologie quantitative.

Il processo di analisi dei rischi:

- ambito dell'analisi
- perimetro e data di riferimento
- metodo di lavoro
- personale coinvolto
- identificazione degli asset e loro valorizzazione.

Data asset.

Hardware asset.

Software asset.

Location Asset.

Human asset.

Case Study.

I modelli degli asset.

Valorizzazione degli asset.

Identificazione delle minacce.

Identificazione delle vulnerabilità.

Identificazione delle contromisure.

Case Study:

- calcolo del rischio assoluto
- calcolo del rischio residuo.

I controlli.

Il processo decisionale.

Le caratteristiche ideali di una metodologia per l'analisi dei rischi.

Case Study.

Obiettivi

Al termine del corso i partecipanti sono in grado di interpretare e mantenere un'Analisi dei Rischi.

Destinatari

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, EDP auditor e analisti di sicurezza.

Prerequisiti

Buona conoscenza delle problematiche di sicurezza logica.



La gestione della Sicurezza dell'Informazione (ISMS): dalla norma ISO IS 27001 all'audit UNI EN ISO 19011

Le informazioni rappresentano beni intangibili che aggiungono valore all'interno di una organizzazione, pertanto è necessario proteggere i dati da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Gli standard di sicurezza delle informazioni introducono una serie di attività che consentono di elevare il livello di sicurezza delle informazioni aziendali in modo sistematico e controllato attraverso la realizzazione di un sistema di gestione (certificabile da parte di Organismi di Certificazione abilitati). La Norma ISO/IEC 27001:2013 è lo standard internazionale di riferimento che fornisce i requisiti per implementare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI o ISMS), efficace e efficiente nel tempo. Il primo ottobre 2013 è stata pubblicata la nuova versione della norma che condensa alcuni controlli ed assume una forma comune ad altri schemi per facilitarne l'integrazione. Il corso si basa sull'analisi di tutti gli aspetti teorici e pratici della norma e sulle tematiche di audit dei sistemi di gestione, corredate da diverse attività pratiche, che permetteranno al discente di avere una conoscenza dell'argomento sul campo, attuando immediatamente, sotto la supervisione del docente, quanto appreso teoricamente.

Agenda (3 giorni)



Introduzione alla gestione della sicurezza dell'informazione.

Finalità dello standard.

Approccio per processi.

Riferimenti normativi.

Termini e definizioni.

Sistema di gestione per la sicurezza delle informazioni:

- contesto dell'organizzazione
- campo di applicazione.

Leadership; Politica; Ruoli, Responsabilità, Autorità della Direzione.

Pianificazione; Valutazione e Trattamento dei rischi relativi alla sicurezza delle informazioni.

Obiettivi per la sicurezza delle informazioni.

Supporto; Gestione delle risorse; Competenza; Consapevolezza; Comunicazione.

Gestione della documentazione del SGSI.

Monitoraggio del SGSI.

Audit interni del SGSI.

Riesame del SGSI da parte della Direzione.

Miglioramento del SGSI:

- non conformità e azioni correttive
- miglioramento continuo.

Allegato A: Obiettivi di controllo e controlli.

Audit dello schema ISO 27001 secondo la norma UNI EN ISO 19011:2012

Prerequisiti di un auditor

Redazione di un piano di audit e redazione di un programma di audit.

Conduzione dell'audit sul campo.

Redazione di un rapporto di audit.

Il ciclo di audit interni.

Le check-list.

Case study ed esercitazioni pratiche.

La gestione della Sicurezza dell'Informazione (ISMS): dalla norma ISO IS 27001 all'audit UNI EN ISO 19011

Obiettivi

Al termine del corso i partecipanti saranno in grado di valutare le attività necessarie per la realizzazione di un SGSI certificabile secondo la norma ISO/IEC 27001:2013 e delle tematiche in tema di audit dei sistemi di gestione. Inoltre, saranno in grado di ricevere un audit sia interno sia esterno.

Destinatari

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, internal auditor, analisti di sicurezza, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti particolari se non di tipo ICT generale e di alcune basi di sicurezza delle informazioni.



Aggiornarsi alla norma ISO/IEC 27001:2013 e tematiche di Audit

L'analisi dei sistemi di gestione o semplicemente di alcuni aspetti contrattuali formalizzati con un fornitore è un aspetto fondamentale per il miglioramento continuo di una specifica area aziendale o di tutta l'azienda nel suo complesso.
Il corso fornisce gli aspetti fondamentali per l'esecuzione sul campo di un audit di prima parte (o interno) e di seconda parte (o esterno) trasmettendo al partecipante le tecniche necessarie e le modalità per lo svolgimento di un audit conformemente alla norma ISO 19011:2012 ("Linee guida per audit di sistemi di gestione"). Questo corso che prepara il partecipante a ricevere un Audit secondo ogni crite si basa prevalentemente su esercitazioni pratiche, che permettono di avere una conoscenza dell'argomento sul campo, attuando immediatamente, sotto la supervisione del docente, quanto appreso nella parte teorica.

Agenda (2 giorni)



Introduzione agli audit.

Termini e definizioni.

Generalità sugli audit di prima, seconda e terza parte.

Finalità dello standard.

Competenze di un auditor.

Definizione di un piano di audit.

Definizione di un programma di audit.

Condivisione di un programma o di un piano di audit.

Il rapporto di chiusura.

Attività di follow up.

Il ciclo di Deming.

I sistemi di gestione.

Il ciclo di audit interni.

Esercitazioni pratiche.

Obiettivi

Al termine del corso i partecipanti saranno in grado di eseguire un audit secondo uno schema definito e conformemente alla norma ISO 19011:2012.

Destinatari

Responsabili della sicurezza informatica, Responsabili di progettazione di sistemi di sicurezza, EDP auditor e analisti di sicurezza.

Prerequisiti

Buona conoscenza delle tematiche inerenti i sistemi di gestione.

Informatica Forense (Computer Forensics): aspetti pratici

Il corso affronta, con un approccio orientato alla sperimentazione, la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in sede processuale.
Al termine del corso si acquisiranno le competenze necessarie al "computer forensic expert" ovvero la figura professionale che presta la sua opera nell'ambito dei reati informatici o del computer crime con lo scopo di "preservare, identificare, studiare ed analizzare i contenuti memorizzati all'interno di qualsiasi supporto o dispositivo di memorizzazione". Le attività sono dirette non solo a tutte le categorie di computer, ma a qualsiasi attrezzatura elettronica con potenzialità di memorizzazione dei dati (ad esempio, cellulari, smartphone, sistemi di domotica, autoveicoli e tutto ciò che contiene dati memorizzati.

Agenda (3 giorni)



Individuazione:

- il primo e più importante passo che un *computer forensic expert* deve compiere prima di iniziare la sua investigazione, è quello di identificare la prova informatica e la sua possibile posizione. Una prova digitale può essere infatti contenuta in diverse tipologie di supporti, come hard disks, media rimuovibili oppure un log file su un server.

Conservazione e Protezione:

- il computer forensic expert deve garantire il massimo impegno per conservare l'integrità della prova informatica. Il dato originale non deve essere modificato e danneggiato e quindi si procede realizzandone una copia (bit-a-bit), su cui il computer forensic expert compie l'analisi. Dopo aver effettuato la copia è necessario verificarne la consistenza rispetto al dato originale: per questo motivo si firmano digitalmente il dato originale e la copia, che devono coincidere.
- esercitazioni in laboratorio su: dd, ddrescue, md5sum, autopsy (calcolo hash e analisi di device).

Estrazione:

- è il processo attraverso il quale il computer forensic expert, servendosi di diverse tecniche e della sua esperienza, trova la posizione del dato informatico ricercato e lo estrae. Verrà fatta una panoramica sui forensics tool Helix, CAINE ed Encase
- esercitazioni in laboratorio su: recupero file cancellati, ricerche su file e settori allocati/non allocati, creazione ed interpretazione della timeline, analisi di pagefile.sys/hiberfile.sys/NTUSER.DAT, funzionamento di Emule, utilizzo dell'analizzatore di protocolli di rete Wireshark.

Documentazione:

- l'intero lavoro del digital forenser deve essere costantemente documentato, a partire dall'inizio dell'investigazione fino al termine del processo. La documentazione prodotta comprende, oltre alla catena di custodia, un'analisi dei dati rinvenuti e del processo seguito. Un'accurata documentazione è di fondamentale importanza per minimizzare le obiezioni e spiegare come ripetere l'estrazione con un analogo processo sulla copia.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare (individuare, estrarre) mediante utilizzo di strumenti open source e documentare con precisione il processo seguito ed i risultati ottenuti.

Destinatari

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

Digital Forensics

La criminalità per far perdere le tracce dei delitti commessi e degli autori coinvolti ricorre sempre più spesso a strumenti informatici. Per contrastare il fenomeno tra gli investigatori cresce la necessità di figure professionali specializzate nella Digital Forensics, la branca della Criminalistica che si occupa dell'identificazione, preservazione e analisi di quanto contenuto nei sistemi informatici o telematici e che evidenzia l'esistenza di fonti di prova digitali che resistano a contestazioni circa la solidità e la capacità probatoria in ambito civile o penale.
La Digital Forensics è una scienza nuova che solo nel febbraio 2008 l'*American Academy of Forensic Sciences* (AAFS) ha inserito nel novero delle scienze riconosciute.
Il corso consente di acquisire le competenze necessarie sia al *Digital Evidence First Responder* (DEFR) che al *Digital Evidence Specialist* (DES) per lo svolgimento delle attività di sopralluogo digitale e di analisi di reperti virtuali.

Agenda (3 giorni)



Introduzione:

- introduzione alla Digital Forensics e al concetto di prova digitale
- standard ISO di riferimento
- legislazione in materia di criminalità informatica.

Il Sopralluogo Digitale:

- attuazione della ISO27037:2012 sulla scena del crimine informatico, attraverso lo studio delle fasi di:
  - Identificazione (*Identification*): ricerca della fonte di prova digitale
  - Acquisizione (*Acquisition*): rilievo tecnico volto a congelare la fonte di prova digitale
  - Repertamento (*Collection*): attività volta ad assicurare la fonte di prova digitale
  - Preservazione (*Preservation*): attività volta a garantire l'integrità e riservatezza della fonte di prova digitale
  - Validazione (*Validation*): conferma che sono stati rispettati i requisiti per i fini d'indagine (principio di pertinenza).

Verifica, Analisi ed Interpretazione dei dati:

- uso di software, preferibilmente Open Source, al fine di attuare le principali tecniche di verifica ed analisi di reperti virtuali, secondo procedure scientificamente derivate dirette a confermare, o confutare, una tesi accusatoria
- l'interpretazione è l'unica fase soggettiva dell'intero processo in cui l'investigatore fornisce valutazioni di merito alla pertinenza con il contesto d'indagine e l'uso dei dati per l'eventuale proseguimento delle indagini.

Documentazione e Presentazione:

- la documentazione è l'insieme di atti e documenti volti a storicizzare le attività svolte. Tale attività è prologo della presentazione, dove lo specialista dovrà aver cura di fornire una giustificazione dell'attinenza con l'indagine della traccia informatica rilevata, ossia fornire un legame logico-deduttivo comprensibile a persone che non hanno un'elevata competenza informatica, come ad esempio Giudice, Pubblico Ministero ed Avvocato.
- la professionalità sia del DEFR che del DES sarà quindi misurata anche nel saper realizzare:
  - una solida Catena di Custodia (*Chain of Custody*), ossia l'insieme di documenti che accompagnano la vita del reperto dalla sua formazione alla sua restituzione all'avente diritto o distruzione
  - un Verbale (art. 134 c.p.p. e seg.) di operazioni tecniche, in caso l'operatore appartenga alla PG
  - Referto tecnico nel caso in cui l'operatore non appartenga alla PG (es. CTU, CTU, Perito).

Cenni sulle Tecniche investigative in internet

- tecniche di OSINT (Open Source Intelligence)
- Sopralluogo Virtuale
- tracciamento.

Digital Forensics

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare nel rispetto dei principi stabiliti sia dal Legislatore italiano (ex L.48/2008) che dai principali standard (ISO 27037 e segg.) e linee guida internazionali (NIST, ...).

Destinatari

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.



Analisi Forense dei Dispositivi Mobili (Mobile Forensics)

Nelle indagini relative alla commissione di reati, sempre più frequentemente, i dispositivi mobili e le tecnologie informatiche - tablet, smartphone, telefono cellulare, navigatore satellitare - forniscono utili indizi alla risoluzione del caso.
La Mobile Forensics è il settore della Digital Forensics che si occupa di recuperare prove digitali, da dispositivi mobili, usando metodi che non compromettano il loro stato probatorio.
Il corso affronta le problematiche inerenti le attività di analisi forense su dispositivi mobili, le procedure per la preservazione, acquisizione, analisi e reporting delle informazioni digitali, utilizzando strumenti open-source e tool proprietari.
Al termine del corso si acquisiscono le competenze necessarie sia come *Digital Evidence First Responder* (DEFR) che *Digital Evidence Specialist* (DES) per poter svolgere analisi approfondite sui sistemi operativi dei più diffusi dispositivi mobili fra cui Android, iOS, Windows Mobile, Windows Phone, Blackberry, Symbian etc.

Agenda (3 giorni)



Introduzione:

- introduzione alla Mobile forensics
- panoramica e caratteristiche sui sistemi operativi più diffusi fra cui Android, iOS, Windows Phone, Windows Mobile, Blackberry, Symbian
- modelli procedurali sulla scienza del crimine.

L’acquisizione:

- le attività invasive – semi invasive e non invasive
- l’acquisizione Fisica
- l’acquisizione Logica
- esercitazioni in laboratorio con strumenti proprietari (XRY, UFED etc.) e tool open-source;
- confronto dei risultati.

Acquisizioni Avanzate:

- l’acquisizione tramite il JTAG
- il Chip-Off: L’acquisizione tramite lettura del chip di memoria da dispositivi danneggiati.

L’analisi dei File Systems:

- il File System FAT/FAT32/EXT/YAFFS2/iOS File System
- file di sistema e Log.

L’analisi dei Database:

- i database di sistema
- text messages (SMS/MMS), Contacts, Call logs, E-mail / Instant Messenger/Chat etc.

Analisi delle Apps:

- i database interni delle App
- i database SQLite.

L’analisi della geolocalizzazione.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare nel rispetto dei principi stabiliti sia dal Legislatore italiano (ex L.48/2008) che dai principali standard (ISO 27037 e segg.) e linee guida internazionali (NIST, ...).

Destinatari

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell’Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

I sistemi di monitoraggio e controllo in rete

Il corso illustra l'evoluzione di sistemi dall'analogico al mondo IP nel modello 3P (dati, voce immagine, sistemi di controllo). In particolare sono affrontate le problematiche relative alla sicurezza di tali sistemi nel passaggio dall'operatività stand-alone alla modalità integrata su rete, mettendo in evidenza: vantaggi, svantaggi, punti deboli e punti di forza.
Sono analizzate le evoluzioni verso IP dei sistemi di telefonia (VoIP), di videosorveglianza (IP-Surveillance), di monitoraggio (antincendio, gestione emergenze, gestione ascensori, monitoraggio processi industriali), di controllo processi (SCADA) e di sicurezza (controllo accessi fisico, antintrusione fisica).

Agenda (3 giorni)

Il modello 3Play.

La sicurezza informatica.

La sicurezza fisica.

I sistemi di monitoraggio e controllo in ambito industriale.

I sistemi di monitoraggio e controllo in ambito territoriale.

La convergenza su IP.

I vantaggi delle soluzioni IP.

La messa in sicurezza logica di sistemi integrati.

Affidabilità e continuità di servizio in ambiente mission critical.

Obiettivi

Formare nuove competenze trasversali che consentano un approccio integrato su IP e sulle tematiche relative alla messa in sicurezza e al monitoraggio di ambienti complessi.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Reti IP. LAN, MAN, Wired e Wireless. Conoscenze di base sulla sicurezza informatica in ambito perimetrale.



La Security dei sistemi di IP-Surveillance

Il corso illustra l'evoluzione di sistemi di videosorveglianza dal mondo analogico al mondo IP. In particolare sono affrontate le problematiche relative alla sicurezza di tali sistemi nel passaggio dalla operatività stand-alone alla modalità integrata su rete, mettendo in evidenza: vantaggi, svantaggi, punti deboli e punti di forza.

Agenda (2 giorni)

I sistemi analogici di videosorveglianza.

La evoluzione in ambiente IP.

Architetture dei sistemi di IP Surveillance.

La sicurezza informatica dei sistemi di IP Surveillance.

Affidabilità e continuità di servizio in ambiente mission critical.

La normativa in vigore sulla Privacy.

Obiettivi

Formare nuove competenze in grado di progettare, implementare e gestire un sistema di videosorveglianza su tecnologia IP e le tematiche relative alla messa in sicurezza come sistema informatico integrato su una rete preesistente.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Reti IP. LAN, MAN, Wired e Wireless. Conoscenze di base sulla sicurezza informatica in ambito perimetrale.

La Cloud Security

La nuova evoluzione dei sistemi informativi porta allo spostamento dei servizi verso centri di erogazione esterni alle organizzazioni. Lavorare in Cloud vuol dire attivare dei servizi applicativi e preoccuparsi solo del loro utilizzo e non della loro gestione sistemistica in termini di Infrastruttura HW/SW o Data Protection. Questo nuovo scenario si innesta ad integrazione del sistema informativo classico basato sul modello server-farm based. Ci si pone come obiettivo la formazione di nuove competenze in grado di progettare, implementare e gestire un sistema di sicurezza informatica in ambiente ibrido, ovvero con parte dei servizi gestiti a livello tradizionale e l'altra parte secondo il paradigma del Cloud Computing. Si rivedono, in quest'ottica, i concetti di sicurezza Classica(logica e perimetrale) e di protezione dei dati.

Agenda (2 giorni)

Il Cloud Computing:

- cenni di virtualizzazione
- architettura ed attori del cloud computing
- i servizi di delivery
    - Infrastructure as a Service
    - Platform as a Service
    - Software as a Service
- i modelli di delivery
    - privato,
    - pubblico
    - ibrido
- la multi-tenancy
- i principali Brand.

Sicurezza delle Informazioni nel Cloud:

- parere del Garante privacy sull'uso del Cloud
- sicurezza del Cloud Provider
- data protection
- Data Lost Prevention
- gli impatti dell'ubicazione del dato nei rapporti transnazionali
- PCI-DSS e Cloud Computing
- sicurezza fisica e logica
    - firewalling
    - autenticazione forte
    - crittografia
    - Business Continuity e Disaster Recovery.

Obiettivi

Formare nuove competenze per progettare, implementare e gestire un sistema di sicurezza informatica in ambiente Cloud Computing.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

DataCenter HW, Sistemi Operativi Enterprise, Storage, Reti (IP, LAN, MAN, Wired e Wireless).
Conoscenze di base sulla sicurezza informatica sia logica che perimetrale.



Realizzare reti sicure con CheckPoint

Il corso affronta i concetti di base per configurare Check Point Security Gateway e Management Software Blades. Gli argomenti su cui verteranno le lezioni sono principalmente le Security Policy e la gestione ed il monitoraggio di una rete sicura. Inoltre, verrà analizzato come configurare il Security Gateway per realizzare una rete privata virtuale per utenti interni, esterni e remoti.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione "Check Point Certified Security Administrator (CCSA-R77)".

Agenda (3 giorni)





Overview sulla tecnologia CheckPoint:

- il Firewall CheckPoint
- meccanismo di controllo del traffico
- architettura del Security Gateway Inspection
- Security Policy Management
- SmartConsole
- Security Management Server.

Piattaforme CheckPoint:

- UTM-1 Edge Appliance
- IP Appliance
- IP Network Voyager
- IPSO
- SecurePlatform.

Security Policy:

- Security Policy Base
- Managing Object
- Rule Based
- Gestione Policy e Revision Control
- NAT.

Monitoraggio del Traffico e delle Connessioni:

- SmartView Tracker
- SmartView Monitor
- Monitoring Sospicius Activity Rules
- Gateway Status.

Smart Update:

- SmartUpdate e Gestione Licenze
- architettura SmartUpdate.

User Management e Authentication:

- Users e Groups
- Security Gateway Authentication
- User Authentication
- Session Authentication
- Client Authentication
- LDAP User Management con SamrtDirectory.

Identity Awareness:

- abilitare l'Identity Awareness
- definizioni di Access Rule.

CheckPoint VPN:

- configurare le VPN
- topologie VPN
- Access Control e VPN Communities
- integrazione di VPN in una Rule Base
- Remote Access VPN.

Realizzare reti sicure con CheckPoint

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dai sistemi Check Point.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazioni Check Point Certified Security Administrator.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.



Realizzare reti sicure con CheckPoint: aspetti avanzati

Il corso affronta i concetti avanzati su Check Point Security Gateway e Management Software Blades. In particolare il corso fornisce una preparazione pratica per ottenere competenze avanzate necessarie per gestire e risolvere i problemi su Check Point R77 Software Blades, tra cui firewall avanzati, gestione avanzate degli utenti e clustering, IPsec e VPN avanzata e accesso remoto. Inoltre, i discenti, andranno ad eseguire il debug sui processi dei firewall e ad ottimizzare le prestazioni della VPN.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione "Check Point Certified Security Expert (CCSE-R77)".

Agenda (3 giorni)





Upgrading Avanzato:

- Back up and Restore Security Gateways
- Workflow
- Upgrade Cluster
- Inter-VDOM link.

Firewall Avanzato:

- Infrastruttura Firewall-1
- Secure Gateway
- Kernel Tables
- NAT
- FW Monitor.

Clustering e Acceleration:

- ClusterXL: Load Balancing
- Gestione HA
- SecureXL: Secure Acceleration
- CoreXL: Multicore Acceleration
- Forwarding Domain.

User Management Avanzato:

- User Management
- Identity Awareness.

IPSec VPN avanzato e Accesso Remoto:

- VPN Azanzate
- VPN per Accesso Remoto
- Multiple Entry Point VPN
- Tunnel Management
- VPN Debug.

Auditing e Reporting:

- Processi di Auditing e Reporting
- SmartEvent
- SmartReporter
- Virtual Clustering.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza avanzati messi a disposizione dai sistemi CheckPoint.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione CheckPoint Certified Security Expert.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di sistemi CheckPoint.



Reti sicure in ambiente Fortinet: aspetti di base

Il corso fornisce le conoscenze necessarie per poter mettere in esercizio e configurare firewall Fortinet. Ciò comporta la capacità di saper configurare dispositivi FortiGate a supporto di specifiche politiche aziendali. Dopo aver illustrato le caratteristiche dei prodotti Fortinet, il corso fornisce tutti gli elementi per una solida comprensione della configurazione e del monitoraggio quotidiano dei dispositivi FortiGate.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione FCNSA – Fortinet Certified Network Security Associate.

Agenda (2 giorni)





User Management Avanzato:
- User Management
- Identity Awareness.

IPSec VPN avanzato e Accesso Remoto: Overview and System Setup:
- La soluzione Fortinet
- Basi di Firewalling
- FortiGate
- Device Adminsitrator.

Servizi FortiGuard:
- FortiGuard Distribution Network
- FortiGuard Antivirus Service
- FortiGuard Intrusion Protection System Service
- FortiGuard Web Filtering Service
- FortiGuard AntiSpam Service.

Logging and Alerts:
- Log Storage Location
- Logging Levels
- Log types
- Configure Logging.

Basic VPN:
- Fortigate VPN
- SSL VPN
- PPTP VPN
- IPSec VPN.

Authentication:
- Metodi di autenticazione
- Utenti e Gruppi di Utenti
- PKI Authentication
- Radius Authentication
- LDAP Authentication
- TACACS+
- Microsoft ActiveDirectory Authentication.

Antivirus:
- Antivirus Elements
- File Filter
- Virus Scan
- Grayware
- Quarantena.

Spam Filtering:

- Metodi di Spam Filtering
- FortiGuard Antispam
- Banned Word
- Black\White List
- Quarantena.

Web Filtering:

- Web Content Block
- Web content Exemption
- URL Filter
- FortiGuard Web Filter.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dagli apparati Fortinet.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione Fortinet FCNSA.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.



Reti sicure in ambiente Fortinet: aspetti avanzati

Il corso fornisce l'expertise necessaria per l'installazione e la configurazione di tutte le caratteristiche e funzionalità dei dispositivi FortiGate. In particolare, i discenti saranno in grado di configurare FortiGates multipli sfruttando le caratteristiche di ambienti di grande scala, quali HA e VPN ridondanti. Le lezioni del corso, oltre ai dispositivi FortiGate, affronteranno anche i prodotti FortiMail, FortiManager e FortiAnalyzer.
Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione FCNSP – Fortinet Certified Network Security Professional.

Agenda (3 giorni)





Virtual Networking:

- Virtual Local Area Network
- Virtual Domain
- Inter-VDOM link.

Diagnostic:

- comandi di Diagnostica
- Self Help Options.

Modalità Trasparent:

- modalità Operative
- Vlan sul Fortigate in modalità Trasparent
- Broadcasting Domain
- Forwarding Domain
- Spanning Tree Protocol
- Link Aggregation.

Firewall Policy:

- firewall Policy
- firewall Addresses
- firewall Schedules
- firewall Services
- firewall Action
- firewall Policy Options
- Virtual IP
- Load Balacing.

Routing:

- Policies di routing, rotte statiche e NAT
- Dynamic Routes
- Multicat Routing.

Ottimizzazione del Traffico:

- tecniche Fortigate per l'ottimizzazione delle WAN
- Web cache
- supporto WCCPv2
- Quality of Service.

Gestione delle minacce:

- tecniche di Scansione dei contetnuti
- componenti architetturali della gestione delle minacce
- Antivirus
- Intrusion Prevention System
- Web Filtering
- Spam Filtering
- Data Leak Prevention
- Application Control
- Network Access Control Quarantine
- SSL Content Ispection.

Reti sicure in ambiente Fortinet: aspetti avanzati

Advanced Authentication:

- Identity-Based Polies
- User Groups
- Authentication Settings
- LDAP Authentication
- Certificate Authentication
- Directory Services Authentication.

Virtual Private Networks:

- SSL VPN
- IPSec VPN
- Internet Key Exchange
- Internet Browsing.

High Availability:

- High Availability cluster
- Protocolli di Clustering FortiGate
- modalità di High Availability
- Failover
- Virtual Clustering.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza avanzati messi a disposizione dagli apparati Fortinet.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione Fortinet FCNSP.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing; uso e configurazione di base di apparati Fortinet. acquisibile tramite il corso Fortinet base.



Unified Access Control: la sicurezza degli endpoint in contesti critici

Le organizzazioni ICT hanno la necessità di ottenere livelli di sicurezza sempre più elevati in modo da garantire allo stesso tempo il business e il rispetto delle normative nazionali e internazionali relative alla protezione delle informazioni. Questi vincoli però si scontrano con le nuove tendenze del mondo ICT che vedono una forte diffusione dei servizi che non sono più relegati a uno stretto gruppo di tecnici. Inoltre negli ultimi anni con il successo dei dispositivi mobili e dell'outsourcing è sparito il tradizionale concetto di perimetro aziendale che determinava il confine logico tra l'azienda e il mondo esterno. La tecnologia Unified Access Control (UAC) di Juniper ha lo scopo di permettere l'accesso degli utenti da qualunque piattaforma (PC,notebook, smart phone, tablet) ai servizi ICT dell'azienda in modo sicuro e controllato. Il corso mira a far acquisire le conoscenze necessarie per il design, configurazione e troubleshooting della tecnologia Unified Access Control (UAC) di Juniper. Gli argomenti illustrati saranno affiancati da attività di laboratorio durante le quali i partecipanti avranno modo di mettere in pratica quanto appreso.

Agenda (3 giorni)



Configurazione iniziale dell'Infranet Controller.

Verifica e Troubleshooting.

Access Management Framework.

Overlay Enforcement.

Layer 3 Secure Access.

Configurazione dell'Overlay Enforcement.

Configurazione del Guest Access.

Server di autenticazione.

Processo di autenticazione.

Configurazione dell'Authentication Servers e configurazione dell'Authentication Realms.

Endpoint Security.

Host Checker.

Configurazione dell'Host Checker.

Remediation.

Layer 2 Enforcement.

802.1X.

RADIUS.

MAC Authentication.

Configurazione del Layer 2 Enforcement.

Configurazione del 802.1X Authenticator.

Configurazione del 802.1X sull'IC.

Configurazione MAC Authentication.

Logging, Monitoring, Troubleshooting Tool.

Obiettivi

Fornire competenze, metodologie e criteri per la gestione dei controlli di accesso attraverso la tecnologia Unified Access Control (UAC) di Juniper.

Destinatari

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base dei Sistemi Informativi, TCP/IP, Sistema operativo Windows.



Reti sicure in ambiente Juniper: aspetti base

Il corso è pensato per i professionisti nell'ambito networking con conoscenze intermedie del software Juniper Network Junos per la serie di dispositivi SRX. Sono analizzate tematiche relative alla configurazione, alle operazioni e alle implementazioni di soluzioni per un ambiente di rete basato su SRX Service Gateway. Gli argomenti chiave, descritti in dettaglio nel programma, includono tecnologie di sicurezza come policy, intrusion detection e prevention, NAT, High Availability cluster, web filtering, antivirus, antispam e filtraggio dei contenuti.
Il corso comprende i temi di "Junos Security (JSEC)" e "Junos Unified Threat Management (JUTM)" e fornisce le competenze necessarie per sostenere l'esame Juniper JN0-332, per la certificazione Juniper Networks Certified Specialist Security (JNCIS-SEC).

Agenda (4 giorni)





Panoramica Junos Security:

- Junos security architecture
- principali componenti hardware degli SRX Service Gateway
- Forwarding packet-based vs. session-based.

Zone:

- tipi di zone
- passi di configurazione delle zone
- ordini di configurazione
- monitoraggio e troubleshooting.

Policy di sicurezza:

- tipi, componenti e ordinamento di policy
- ispezione del traffico diretto al dispositivo e del traffico in transito
- Scheduling
- Rematching
- Application Level Gateway
- Address books
- applicazioni
- passi di configurazione delle policy
- configurazione applicazioni custom
- monitoraggio e troubleshooting.

Firewall User Authentication:

- tipi di autenticazioni utente
- supporto server di autenticazione
- Client groups.

Screen:

- opzioni di screen
- passi di configurazione degli screen
- monitoraggio e troubleshooting.

NAT:

- tipi di NAT/PAT
- linee guida alla configurazione
- passi di configurazione del NAT
- monitoraggio e troubleshooting.

VPN IPSec:

- caratteristiche e componenti delle secure VPN
- opzioni di implementazione di Junos OS per IPSec
- passi di configurazione delle VPN IPSec
- monitoraggio e troubleshooting.

Reti sicure in ambiente Juniper: aspetti base

High Availability (HA) Clustering:
- caratteristiche e componenti della HA
- modalità di cluster
- stato di sincronizzazione
- preparazione del cluster
- passi di configurazione del cluster
- monitoraggio e troubleshooting.

Unified Threat Management (UTM):
- Policy di flusso
- supporto alla piattaforma
- Licensing.

Filtro Antispam:
- soluzioni antispam
- Whitelist vs. blacklist
- ordine delle operazioni
- analisi del traffico
- passi di configurazione usando la CLI
- monitoraggio e troubleshooting.

Protezione Antivirus:
- metodi di scanning
- passi di configurazione usando la CLI
- monitoraggio e troubleshooting.

Web Filtering:
- caratteristiche e soluzioni di filtering
- passi di configurazione usando la CLI
- monitoraggio e troubleshooting.

Obiettivi

Al termine del corso i partecipanti saranno in grado di valutare e attivare i vari meccanismi di sicurezza – firewall, VPN, filtraggio dei contenuti – messi a disposizione dal Junos OS dei router, degli switch e dei dispositivi della serie SRX.

Destinatari

Amministratori di rete, responsabili della sicurezza di rete, consulenti di sicurezza, responsabili dell'implementazione di reti sicure di piccole/medie dimensioni.
Candidati al conseguimento della certificazione Juniper JN0-332.

Prerequisiti

Conoscenze di base su stack di protocolli TCP/IP, principi di base di sicurezza sulle reti, principi di base su switching e routing in ambiente Juniper e uso e configurazione di base di apparati Juniper



Reti sicure in ambiente Juniper: aspetti avanzati

Il corso è pensato per i professionisti nell'ambito networking con conoscenze avanzate del software Juniper Network Junos per la serie di dispositivi SRX. Verranno coperti argomenti avanzati relativi alla configurazione, al monitoraggio e alle implementazioni di soluzioni Junos OS per la sicurezza. Gli argomenti chiave sono descritti di seguito nel dettaglio ed includono tecnologie di sicurezza come IPSec, virtualizzazione, AppSecure, NAT avanzato, sicurezza layer 2 e IPS.
Il corso comprende i temi di "Advanced Junos Security (AJSEC)" e "Junos Intrusion Prevention System Functionality (JIPS)" e fornisce le competenze necessarie per sostenere l'esame Juniper JNO-633, per la certificazione Juniper Networks Certified Professional Security (JNCIP-SEC).

Agenda (5 giorni)





Servizi di sicurezza application-aware:

- elaborazione del traffico AppSecure
- AppID
- AppTrack
- AppFW
- AppDoS
- AppQoS.

Virtualizzazione:

- istanze di routing
- Gruppi RIB
- Routing tra istanze diverse
- Logical systems (LSYS)
- comunicazione Intra-LSYS e Inter-LSYS
- Filter-based forwarding (FBF).

NAT avanzato:

- elaborazione del traffico NAT
- NAT sulla destinazione
- NAT sulla sorgente
- NAT persistente
- NAT statico
- doppio NAT
- NAT trasversale
- DNS doctoring
- NAT IPv6 (Carrier-grade NAT) - NAT64, NAT46, NAT444, DS-Lite
- Routing
- NAT e FBF
- NAT e policy di sicurezza.

VPN IPSec avanzate:

- elaborazione del traffico IPSec
- VPN site-to-site
- VPN hub-and-spoke
- VPN di gruppo
- VPN dinamiche
- Routing su VPN
- VPN e NAT
- Public key infrastructure (PKI) per VPN IPSec
- VPN e dynamic gateways.

Reti sicure in ambiente Juniper: aspetti avanzati

Intrusion Prevention:

- processo di ispezione pacchetti IPS
- IPS role-based
- rilevamento degli attacchi signature-based
- riconoscimento scansioni e impronte digitali
- Flooding, attacchi e spoofing
- opzioni di deployment degli IPS e considerazioni
- impostazioni di rete
- database di attacchi
- Signature personalizzate
- prevenzione dello scan.

Transparent Mode:

- High Availability
- traduzione VLAN
- Sicurezza layer 2
- IRB
- Bridge groups
- Elaborazione del traffico Spanning tree.

Troubleshooting:

- analisi di flusso
- SNMP
- Show commands
- Logging e syslog
- Tracing, incluso flow traceoptions
- Policy di flusso
- cattura di pacchetti.

Obiettivi

Al termine del corso i partecipanti saranno in grado di valutare e attivare i vari meccanismi avanzati di sicurezza – NAT, VPN, IPSec, IPS – messi a disposizione dal Junos OS dei router, degli switch e dei dispositivi della serie SRX.

Destinatari

Amministratori di rete, responsabili della sicurezza di rete, consulenti di sicurezza, responsabili dell'implementazione di reti sicure di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JN0-633.

Prerequisiti

Conoscenze di sicurezza sulle reti, sull'uso degli apparati della serie SRX, sull'uso e la configurazione di apparati di rete Juniper.

CCNA Security

Il corso CCNA Security fornisce le competenze necessarie per amministrare in sicurezza una rete IP di medie dimensioni sia in ambito LAN che WAN. L'obiettivo del corso è quello di preparare i partecipanti a diventare delle figure professionali in grado di sviluppare una infrastruttura sicura di rete, di valutare le vulnerabilità della propria rete e di mettere in campo le opportune misure per contrastare le possibili minacce.
***Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco* 640-554 IINS v2.0.**

Agenda (5 giorni)





Le componenti tecniche del "Sistema-Sicurezza":

- disponibilità, integrità (autenticità, non-ripudio), Riservatezza
- sicurezza logica: servizi di sicurezza, tipologia degli attacchi, anatomia di un attacco
- certificare la sicurezza (ISO 27000 e ISO 15408).

Esaminare le tipologie di attacco e minimizzare la probabilità di successo dell'attacco:

- mitigare gli attacchi di accesso abusivo
- attacchi basati sulle password
- sfruttamento della fiducia (trust exploitation)
- redirezione delle porte
- mitigare gli attacchi di Buffer Overflow
- IP Spoofing
- attacchi DoS e DDoS
- virus, worm, e trojan horse
- attacchi a livello applicativo
- protocolli di gestione
- attacchi di raccolta delle informazioni (reconnaissance)
- packet sniffer; port scan e ping sweep; query alla Internet pubblica.

Rendere sicuro l'accesso amministrativo degli apparati di rete:

- configurare la password
- creazione di un account utente
- configurare Role-Based CLI access
- configurare il supporto avanzato per Virtual Login.

Sicurezza nei router Cisco:

- come mettere in sicurezza il piano dei dati, di controllo e di management
- descrivere Cisco Security Manager
- descrivere le implicazioni che IPv6 introduce nel campo della sicurezza.

Configurare AAA sui Router Cisco usando il database locale:

- descrivere le funzioni e l'importanza di AAA
- conoscere come i servizi di AAA (Authentication, Authorization, Accounting) sono supportati in Cisco IOS software
- conoscere come rendere sicuro l'accesso ai dispositivi di rete e alle reti
- configurare AAA con un database locale.

Configurare AAA con l'ausilio di Cisco Secure ACS:

- comprendere i benefici di un AAA centralizzato
- conoscere le caratteristiche di Cisco Secure Acces Control Server (ACS)
- conoscere le caratteristiche dei protocolli RADIUS e TACACS+
- installare e configurare il server ACS
- configurare i protocolli RADIUS e TACACS+
- verificare l'operatività di AAA (troubleshooting).

Liste di accesso:

- access control lists (ACL)
- standard IP ACL e Extended IP ACL
- gestione avanzata delle ACL
- configurare e verificare le ACL.

Gestione sicura degli apparati e monitoraggio:

- gestione In-Band e Out-Band
- linee guida generali sul Management e Reporting in sicurezza
- usare i log per monitorare la sicurezza della rete; modelli e livelli di sicurezza di SNMP
- Secure Shell (SSH).

Attacchi a livello 2:

- proteggere le funzionalità di inoltro degli switch: MAC flooding, MAC spoofing
- port security
- prevenire il VLAN hopping: switch spoofing, doppio tag
- prevenire le manipolazioni dello STP: BPDU guard, root guard, BPDU filtering
- proteggere il DHCP
- Private VLAN
- monitoraggio su reti switched (SPAN: Switched Port Analyzer).

Tecnologie di firewalling:

- soluzioni per la difesa del perimetro della rete aziendale
- funzionalità di un firewall: packet filtering, proxy, statefull inspection
- funzionalità complementari
- architetture firewall: screened host, screened network o subnet (DMZ)
- tipi di NAT usati nei firewall
- configurare Network Address Translation (NAT) e Port Address Translation (PAT)
- configurare Cisco IOS Zone-Based Policy Firewall usando CCP (Cisco Configuration Professional)
- case studies su Zone-based firewall
- apparati Cisco di firewalling: Adaptive Security Appliance (ASA).

Cisco IPS:

- descrivere le funzioni di Cisco Intrusion Prevention System (IPS)
- tecnologie IPS: Profile-based, Signature-based, Protocol-based
- mitigazione delle minacce su un sistema distribuito utilizzando IPS
- configurare Cisco IOS IPS usando CCP (Cisco Configuration Professional).

IPSec e VPN:

- strumenti per la sicurezza dei dati, crittografia pratica
    - crittografia simmetrica o a chiave segreta
    - crittografia asimmetrica o a chiave pubblica
    - funzioni di hashing (MD5, SHA-1) ed HMAC
    - certificati Digitali e PKI
- reti private virtuali (RPV o VPN): tipi e tecnologie
- componenti e funzionalità di IPSec: AH, ESP e IKE
- configurare IPSec site-to-site con chiavi precondivise
- verificare l'operatività delle VPN
- realizzare VPN con Secure Sockets Layer (SSL).

Simulazione dell'esame e test di preparazione.

Obiettivi

Fornire le conoscenze e competenze necessarie per l'installazione, la gestione ed il troubleshooting dei dispositivi di rete garantendo il mantenimento dell'integrità, della disponibilità e della riservatezza delle informazioni gestite dalla rete.

Destinatari

Tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti IP che vogliono minimizzare l'impatto che malfunzionamenti, provocati o accidentali, possono causare sulla propria rete IP.

Prerequisiti

Sono richieste nozioni sull'internetworking simili a quelle fornite nel corso CCNA: conoscenze sui concetti e i termini legati al mondo del networking e dell' IP, conoscenza del mondo LANs, WANs, e IP switching/ routing, capacità di configurare un router e uno switch con la CLI.



Reti sicure in ambiente Cisco, difesa perimetrale con IOS e ASA

Il corso affronta le tematiche della sicurezza perimetrale di rete, in particolare come configurare e implementare le policy che apparati Cisco - router e ASA – devono imporre nei punti perimetrali esterni ed interni . Gli argomenti su cui verteranno le lezioni sono principalmente le tecnologie utilizzate per rafforzare la sicurezza del perimetro di una rete: Network Address Translation (NAT), policy e application inspect degli ASA, e firewall zone-based su router Cisco.
È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Edge Network Security Solutions (SENSS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 300-206 SENSS.

Agenda (5 giorni)





Principi di progettazione di Sicurezza:

- zone di Sicurezza
- architetture modulari
- architettura SecureX
- soluzione TrustSec.

Sviluppo di protezione dell'infrastrutture di Rete:

- sicurezza sul control plane Cisco IOS
- sicurezza sul Management plane Cisco IOS
- sicurezza sul Management plane Cisco ASA
- sicurezza a livello 2
- sicurezza a livello 3.

NAT su Cisco IOS e ASA:

- il NAT (Network Address Traslation)
- implementare il NAT su Cisco ASA
- implementare il NAT su Cisco IOS.

Controlli delle minacce sul Cisco ASA:

- introduzione sul controllo di minacce sul Firewall Cisco
- implementare policy base su Cisco ASA
- implementare policy avanzate su Cisco ASA
- implementare policy Reputation-based su Cisco ASA
- implementare policy Identity-based su Cisco ASA.

Controlli delle minacce su Cisco IOS:

- implementare policy base su Cisco IOS
- implementare policy avanzate su Cisco IOS.

Obiettivi

L'obiettivo del corso è quello di fornire agli studenti le conoscenze fondamentali e le capacità per attuare e gestire la sicurezza delle reti tramite Firewall ASA, router e switch Cisco.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.



Reti sicure in ambiente Cisco, difesa perimetrale avanzata con ASA

Il corso affronta le tematiche della sicurezza di rete, in particolare, l'architettura avanzata del firewall e la configurazione dei Cisco ASA next-generation firewall, utilizzando policy di accesso e di identità. Gli argomenti su cui verteranno le lezioni sono principalmente gli Intrusion Prevention System (IPS) e i componenti firewall context-aware, così come soluzioni di sicurezza Web (Cloud) e Email Security.
È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Threat Control Solutions (SITCS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-207 SITCS.

Agenda (5 giorni)





Cisco ASA Next-Generation Firewall (NGFW):

- Cisco ASA NGFW
- architettura Cisco ASA NGFW
- Implementare Policy Objects su ASA NGFW
- monitoring del Cisco ASA NGFW
- implementare access policies su Cisco ASA NGFW
- implementare identity policies su Cisco ASA NGFW
- implementare decryption policies su Cisco ASA NGFW.

Cisco Web Security Appliance:

- soluzioni Cisco Web Security appliance
- integrazioni con Cisco Web Security appliance
- implementare controlli di Authentication e identities sul Cisco Web Security appliance
- implementare controlli anty-malware su Cisco Web Security appliance
- implementare Cisco Web Security appliance Decryption
- implementare Cisco Web Security appliance Data Security controls.

Cisco Cloud Web Security:

- Soluzioni Cisco Cloud Web Security
- Configurare Cisco Cloud Web Security
- Web Filtering Policy su Cisco ScanCenter.

Cisco Email Security:

- Soluzioni Cisco Email Security
- Implementare componenti base del Cisco Email Security Appliance
- implementare policies di Incoming e Outcoming del Cisco Email Security Appliance.

Cisco Intrusion Prevention System:

- soluzioni Cisco IPS
- integrazione del sensore Cisco IPS nella rete
- configurazione base del Cisco IPS
- tuning del Cisco IPS
- configurazioni personalizzate delle signaures IPS
- configurare le Anomaly Detection nel Cisco IPS
- configurare le Cisco IPS Reputation-Based.

Obiettivi

Al termine del corso, gli studenti saranno in grado di ridurre il rischio per le proprie infrastrutture IT e le applicazioni che utilizzano funzionalità di appliance di sicurezza con Cisco Firewall Next Generation e fornire supporto operativo per Intrusion Prevention Systems, Web e Email Security.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Reti sicure in ambiente Cisco, identificazione ed accessi sicuri

Il corso affronta l'implementazione dell'architettura di Secure Access Solution, utilizzando 802.1X e Cisco TrustSec. Nel dettaglio viene approfondita la conoscenza della soluzione architetturale Cisco Identity Services Engine (ISE) e i loro componenti come soluzioni complessive di mitigazione delle minacce di rete e di controllo degli endpoint. Il corso comprende anche i concetti fondamentali per integrare dispositivi esterni (BYOD) con il profiling servizi di ISE.
È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Secure Access Solutions (SISAS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-208 SISAS.

Agenda (5 giorni)





Mitigazione delle minacce tramite servizi Identificativi:

- Servizi identificativi
- 802.1x e EAP
- il sistema d'identificazione.

Cisco ISE:

- Cisco ISE
- Cisco ISE PKI
- Cisco ISE Authentication
- Cisco ISE External Authentication.

Controlli di accesso avanzati:

- autenticazione Certified-based
- autorizzazione
- Cisco TrustSec and MACsec.

Autenticazione web e Guest Access:

- implementare WebAuth
- implementare Servizi Guest
- implementare policy avanzate su Cisco ASA
- implementare policy Reputation-based su Cisco ASA
- implementare policy Identity-based su Cisco ASA.

Miglioramenti dei Controlli d'accesso degli Endpoint:

- Implementare le caratteristiche dei servizi
- Implementare i profili dei servizi
- implementare BYOD.

Troubleshooting dei controlli d'accesso.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza degli accessi tramite firewall ASA o IOS dei router e degli switch.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.



Reti sicure in ambiente Cisco, connessioni remote e VPN

Il corso affronta le tematiche della sicurezza di rete, in particolare, come configurare e implementare le soluzioni Virtual Private Network (VPN) che Cisco ha a disposizione sul firewall Cisco ASA e sulle piattaforme software Cisco IOS. Gli argomenti su cui verteranno le lezioni forniranno le conoscenze necessarie per attuare correttamente le comunicazioni a distanza ad alta sicurezza attraverso la tecnologia VPN, come ad esempio l'accesso remoto SSL VPN e site-to-site VPN (DMVPN, FlexVPN).
È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Secure Mobility Solutions (SIMOS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-209 SIMOS.

Agenda (5 giorni)





Fondamenti di crittografia e Tecnologia VPN:

- il ruolo delle VPN nella sicurezza della rete
- VPN e crittografia.

Implementare IPsec point-to-point su Cisco ASA:

- Soluzioni Cisco Secure site-to-site
- implementare VPN IPsec point-to-point con Cisco IOS FlexVPN
- implementare VPN IPsec Hub-and-spoke con Cisco IOS FlexVPN.

Implementare clientless SSL VPNs:

- implementare Clientless SSL VPNs
- implementare Clientless SSL VPNs su Cisco ASA
- implementare applicazioni di accesso per clientless su Cisco ASA
- implementare Authentication and Authorization avanzata per clientless VPN SSL
- implementare policy Identity-based su Cisco ASA.

Implementare Cisco AnyConnect VPN:

- implementare AnyConnect SSL VPN base su Cisco ASA
- implementare AnyConnect SSL VPN azanzato su Cisco ASA
- implementare Authentication e Authorization su Cisco AnyConnect VPN
- implementare Cisco VPN AnyConnect IPSec/IKEv2.

Implementare sicurezza sugli Endpoint e Access Policy dinamiche:

- implementare Host Scan
- implementare DAP per VPN SSL.

Obiettivi

Al termine del corso i partecipanti avranno le conoscenze necessarie per attuare correttamente le connessioni remote ad alta sicurezza attraverso la tecnologia VPN.

Destinatari

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Tecnologie per la mobilità: dal GSM all'UMTS e HSPA fino a LTE

L'introduzione delle tecnologie per la mobilità ha rappresentato, nelle telecomunicazioni, un'autentica rivoluzione. Le tecnologie analogiche, come il TACS prima, e poi quelle digitali, in particolare il GSM, hanno dato un impulso determinante alla diffusione del concetto di mobilità di accesso ai servizi di fonia. L'interesse per i servizi multimediali, soprattutto grazie alla diffusione di Internet, ha favorito l'evoluzione delle tecnologie di tipo "voice centric" verso modalità più efficienti per la trasmissione dati, quali il GPRS e l'EDGE, fino ad arrivare alla terza generazione, l'UMTS, che nasce già come sistema orientato al multimedia. Sviluppo tecnologico e il mercato dei servizi mobili presentano un dinamismo come pochi altri al confronto, ed infatti subito dopo l'evoluzione dell'UMTS, l'HSPA, è praticamente pronta la quarta generazione: LTE.

Agenda (5 giorni)

Introduzione alla propagazione radioelettrica

Introduzione ai sistemi radiomobili cellulari:

- tecniche di accesso multiplo
- tecniche di duplexing.

Criteri di pianificazione cellulare.

Architettura di una rete radiomobile.

Gestione della mobilità.

Localizzazione.

Handover.

Il GSM: trasmissione radio e gestione dei servizi.

Tecniche di sicurezza.

Roaming ed aspetti di tariffazione.

Il GPRS (caratteristiche tecniche e prestazioni).

EDGE (caratteristiche tecniche e prestazioni).

L'UMTS:

- l'interfaccia radio UMTS
- copertura cellulare
- l'UTRAN: architettura
- handover e macrodiversità
- tecniche di controllo di potenza
- evoluzione della core network UMTS.

HSPA High Speed Downlink Racket Access e HSPA+.

La quarta generazione – LTE:

- interfaccia radio
- architettura di rete.

IMS (IP Multimedia Subsystem).

Evoluzione della sicurezza nei sistemi radiomobili.

Obiettivi

Fornire una panoramica completa del processo evolutivo dei sistemi radiomobili cellulari attraverso la descrizione delle varie tecnologie, dalle caratteristiche dell'accesso radio, dell'architettura di rete fino agli scenari di servizio.

Destinatari

Personale tecnico e non tecnico di operatori di TLC, Service Providers e aziende manifatturiere.

Prerequisiti

Conoscenze di base delle reti di TLC e della trasmissione dati



I sistemi radiomobili per non tecnici: dal GSM a LTE

Le tecnologie analogiche come il TACS e, in seguito, quelle digitali come il GSM hanno dato un impulso determinante alla diffusione del concetto di mobilità di accesso ai servizi di fonia. La crescita dei servizi multimediali, con la diffusione di Internet, ha favorito il progredire delle tecnologie di tipo "voice centric" verso modalità più efficienti per la trasmissione dati, quali il GPRS e l'EDGE, fino ad arrivare all'UMTS, che nasce già come sistema orientato al multimedia. Sviluppo tecnologico e mercato presentano un dinamismo come in pochi altri settori e dopo l'evoluzione dell'UMTS, l'HSPA, è già pronta la quarta generazione: LTE.

Agenda (3 giorni)

Introduzione alla propagazione radioelettrica.

Introduzione ai sistemi radiomobili cellulari.

Criteri di pianificazione cellulare.

Architettura di una rete radiomobile.

Gestione della mobilità. Localizzazione. Handover.

Il GSM: trasmissione radio e gestione dei servizi.

Il GPRS (caratteristiche tecniche e prestazioni).

EDGE (caratteristiche tecniche e prestazioni).

L'UMTS (architettura e servizi).

HSPA High Speed Downlink Racket Access e HSPA+.

LTE (interfaccia e architettura).

Obiettivi

Fornire una panoramica completa dei sistemi radiomobili cellulari.

Destinatari

Personale non tecnico.

Prerequisiti

Conoscenze di base delle TLC.



Evoluzione dei sistemi Radiomobili: verso la quarta generazione

Il corso descrive le linee evolutive delle tecnologie per la mobilità, partendo dalle reti orientate alla voce, quali il GSM, per arrivare alle attuali reti multimediali, il 3G e le sue evoluzioni. Il punto di approdo finale e centrale nell'economia del corso è la tecnologia LTE, le sue caratteristiche principali, le innovazioni rispetto ai precedenti sistemi mobili, le prestazioni ottenibili e l'implementazione sul campo. Saranno illustrati quindi gli impatti in rete, sia nella parte radio, che in quella di core network, con particolare attenzione alla sezione di backhauling. Infine sono accennate le implicazioni che l'implementazione delle reti di nuova generazione produrrà sui servizi presenti e futuri.

Agenda (1 giorno)

Architettura di una rete radiomobile.

Gestione della mobilità:

- localizzazione
- Handover.

Il GSM: trasmissione radio e gestione dei servizi.

Il GPRS (caratteristiche tecniche e prestazioni).

EDGE (caratteristiche tecniche e prestazioni).

L'UMTS:

- l'interfaccia radio UMTS
- l'utran: architettura
- evoluzione della core network UMTS
- servizi UMTS.

HSPA High Speed Packet Access.

Verso la quarta generazione: LTE Long Term Evolution:

- e-UTRAN
- EPC Evolved Racket Core
- impatti in rete di LTE (parte radio, backhauling, backbone)
- scenari di servizio per LTE: nuove opportunità e minacce per i servizi esistenti.

Obiettivi

Presentare le caratteristiche fondamentali delle tecnologie per la mobilità.
Evidenziare l'evoluzione tecnologica delle reti radiomobili dalla fonia al multimedia.
Analizzare gli impatti in rete e gli scenari di servizio di LTE.

Destinatari

Personale tecnico e non tecnico di operatori di TLC e aziende manifatturiere, specialisti ICT.

Prerequisiti

Conoscenze di base delle reti di TLC e della trasmissione dati.



UMTS: la terza generazione delle reti mobili ed evoluzioni verso la quarta generazione

I sistemi 3G hanno rappresentato una grande novità nel mondo dei sistemi radiomobili sia da un punto di vista tecnologico, con la introduzione della tecnica CDMA, che di servizio, con il supporto delle applicazioni multimediali. Tuttavia l'evoluzione del mercato e della tecnologia non si ferma mai e quindi c'è già in campo l'HSPA e si parla sempre più concretamente di quarta generazione.
Il corso illustra le caratteristiche tecniche del sistema UMTS, sia nell'interfaccia radio, sia nella evoluzione della architettura di rete, per poi evidenziare le novità evolutive della tecnologia HSPA. Infine si accenna ai trend verso la quarta generazione, analizzando quali potranno essere le caratteristiche dei prossimi sistemi radiomobili.

Agenda (4 giorni)

L'interfaccia radio UMTS:
- l'allocazione della banda UMTS
- le tecniche di accesso
- il CDMA E IL W-CDMA
- la proposta FDD-CDMA
- cenni alla proposta TDD-CDMA
- i canali UMTS.

Copertura cellulare:
- copertura gerarchica
- cell breathing
- tecniche di pianificazione cellulare.

L'UTRAN: architettura.

Handover e macrodiversità.

Tecniche di controllo di potenza.

La core network UMTS:
- releaese 99: reti a circuito e a pacchetto sovrapposte
- release 4 e 5
- evoluzione degli apparati UMTS.

Servizi UMTS.

HSPA High Speed Downlink Racket Access:
- HSDPA
- HSUPA

Tecniche MIMO

HSPA+.

Verso la quarta generazione - LTE:
- interfaccia radio
- modulazione OFDM
- tecniche di accesso multiplo: OFDMA E SC-FDMA
- architetture di rete.

Obiettivi

Illustrare le peculiarità dell'UMTS rispetto alle precedenti tecnologie radiomobili.
Fornire un quadro prospettico delle possibili linee evolutive verso la quarta generazione.

Destinatari

Ingegneri e tecnici di rete, professionisti ICT.

Prerequisiti

Conoscenze di base sulle reti di TLC e sui sistemi radiomobili.



La segnalazione nelle reti 3G e sue evoluzioni

Il corso illustra i diversi protocolli di segnalazione che interessano la rete UMTS, con particolare riferimento alla parte di core network. Dal modello di architettura separata Circuit Switched e Packet Switched di Release 4 si giunge fino al modello All IP della Release 5 e alle successive evoluzioni.

Agenda (4 giorni)

Brevi richiami all'architettura di rete UMTS.

La segnalazione nella rete d'accesso radio (UTRAN).

La segnalazione nel dominio CS:

- elementi di rete del dominio CS
- interfacce
- trasporto della segnalazione CCS7 su IP
- SIGTRAN
- controllo del MGW
- segnalazione tra MGW.

La segnalazione nel dominio PS:

- la segnalazione tra RNC e 3G-SGSN
- i collegamenti di segnalazione nell'interfaccia Iu-PS
- procedura RAB Assignment per l'attivazione di un PDP Context.

Caratteristiche dell'interfaccia Gn:

- architettura del Backbone IP
- utilizzo di Switch Ethernet per collegare gli elementi di rete del backbone IP
- utilizzo di Router per collegare gli elementi di rete del backbone IP
- il ruolo del server DNS
- elementi di interconnessione di reti esterne: Border Gateway
- il protocollo GPRS Tunneling Protocol (GTP)
- procedura di Context Activation.

Caratteristiche dell'interfaccia Gi:

- modalità di assegnazione degli indirizzi IP
- funzioni del server RADIUS
- traduzione degli indirizzi IP privati in indirizzi IP pubblici: modalità statica
- NAT e hide NAT
- il ruolo dei server Proxy e dei firewall
- caratteristiche principali delle VPN (Virtual Private Networks)
- modello Overlay: Tunnelling
- protocollo GRE (Generic Routing Encapsulation)
- modalità IPSec.

Analisi sui tracciati delle principali procedure di segnalazione.

Obiettivi

Comprendere la configurazione dei protocolli di segnalazione nelle reti radiomobili per servizi multimediali.

Destinatari

Ingegneri e tecnici di rete, professionisti ICT.

Prerequisiti

Conoscenza dei sistemi radiomobili e dei protocolli TCP/IP.



Multi Environment Networks: evoluzione e integrazione delle tecnologie wireless

Negli ultimi anni si è avuto un proliferare di tecnologie di comunicazione via radio, terrestri e satellitari, sia per accesso fisso che mobile. Esse non sono da considerare alternative, ma complementari, pertanto si assiste ad uno scenario di interessante integrazione fra le differenti proposte wireless, soprattutto fra quelle a corto, medio e lungo raggio e fra quelle per accesso fisso e mobile.
Il corso fornisce una panoramica delle diverse tecnologie di accesso radio, si evidenziano le differenze prestazionali, applicative e le prospettive di integrazione in ottica della convergenza di servizi e reti verso una "molteplicità di tecnologie di accesso" per i nuovi scenari di servizio. Si accenna, infine, alle possibilità di integrazione fra le tecnologie wireless e quelle di accesso via cavo.

Agenda (3 giorni)

Richiami sulla trasmissione radio.

Le reti a corto raggio:

- reti ad hoc
- reti di sensori
- WPAN
- Bluetooth: tecnologia e applicazioni
- Zig Bee: tecnologia e applicazioni
- WiMedia: tecnologia e applicazioni.

Le WLAN:

- principi di funzionamento
- Wi-Fi
- livello fisico e livello MAC
- principali applicazioni.

WMAN:

- il problema dell'ultimo miglio ed il "Wireless Local Loop"
- WiMax: aspetti radio e architettura di rete.

Evoluzione dei sistemi radiomobili:

- il GSM: architettura di rete e servizi
- il GPRS: architettura di rete e servizi
- l'UMTS: architettura di rete e servizi
- HSPA
- LTE
- Mobile Wi-Max.

Cenni alle tecnologie via satellite:

- sistemi satellitari per telefonia mobile
- sistemi satellitari per servizi multimediali.

Integrazione fra le reti a corto raggio e le reti metropolitane.

Integrazione fisso-mobile: modalità e prospettive.

Integrazione wireless-wired: esempi e possibili sviluppi.

Obiettivi

Fornire una visione completa di tutte le tecnologie wireless disponibili. Analizzare i possibili ambiti applicativi e gli scenari di integrazione.

Destinatari

Personale tecnico e non tecnico di operatori di TLC e aziende manifatturiere, specialisti ICT.

Prerequisiti

Conoscenze tecniche di base sulle reti di telecomunicazione e sulle problematiche della trasmissione radio.

Wi-Fi e Wi-Max

Negli ultimi anni le tecnologie wireless a medio lungo raggio stanno riscuotendo notevole interesse per molteplici applicazioni: dalla copertura indoor di ambienti o interi edifici, fino alla fornitura di servizi a larga banda in ambito metropolitano, in alternativa, o complemento rispetto alle tradizionali metodologie via cavo.
Il corso inizia dalla tecnologia delle Wireless LAN; vengono illustrati i vari standard con focalizzazione su IEEE 802.11, meglio noto come Wi-Fi e sono fornite le specifiche tecniche di tipo trasmissivo e architetturale. Particolare enfasi viene data alle applicazioni commerciali e ai servizi supportati. Si passa poi a quella che può essere considerata un'estensione del Wi-Fi in ambito metropolitano e cioè il Wi-Max, tema, oggi, di grande attualità. Dal concetto generale di Wireless Local Loop, si entra nel dettaglio dello standard IEEE 802.16, descrivendone le caratteristiche trasmissive, le architetture di rete, le prestazioni e le possibili applicazioni.

Agenda (2 giorni)

Le Wireless LAN:

- caratteristiche di una rete locale wireless
- gli standard 802.11
- l'interfaccia radio: livello 1 e 2
- evoluzione degli standard
- caratteristiche degli apparati.

Aspetti commerciali: le molteplici applicazioni del wi-fi.

Integrazione del Wi-Fi con altri sistemi:

- integrazione con le tecnologie radiomobili
- integrazione con le tecniche di accesso fisse.

La mobilità nel Wi-Fi.

Il problema della sicurezza dell'accesso e della riservatezza dei dati.

Wi-Max:

- il WLL e differenze con il Wi-Fi
- evoluzione degli standard
- lo standard 802.16
- prestazioni e confronto con tecniche di accesso via cavo
- lo standard 802.16e: il Wi-Max per la mobilità
- tecniche di copertura cellulare
- il Wi-Max in Italia: la gara per le frequenze e esempi di offerte commerciali
- integrazione con il altre tecnologie d'accesso a larga banda.

La sicurezza nel Wi-Max.

Obiettivi

Illustrare gli aspetti principali delle tecnologie wireless più diffuse in ambito locale e metropolitano.

Destinatari

Personale tecnico e non tecnico di operatori di TLC e aziende manifatturiere, specialisti ICT.

Prerequisiti

Conoscenze di base sulle reti per dati, sui protocolli Ethernet e IP.



Wireless LAN

La tecnologia delle Wireless LAN è andata ben oltre l'iniziale interesse alla realizzazione di una rete locale senza fili. Oggi lo standard più affermato, il Wi-Fi, trova molteplici applicazioni, sia in ambito privato che pubblico, come alternativa o complemento alle tradizionali reti in cavo, sia nel segmento locale che metropolitano, fino a proporsi come alternativa ai tradizionali ponti radio, per la costituzione di vere e proprie dorsali wireless a basso costo. Il corso illustra le caratteristiche generali delle Wireless LAN, vengono illustrati i vari standard con particolare approfondimento su IEEE 802.11, meglio noto come Wi-Fi, e sulle sue evoluzioni. Ne vengono fornite le specifiche tecniche, sia di tipo trasmissivo che architetturale. Particolare enfasi viene data alle applicazioni commerciali e ai servizi supportati.È prevista anche una parte pratica dedicata alla configurazione degli apparati e alla progettazione di una copertura radio attraverso una Wireless LAN.

Agenda (3 giorni)

Le Wireless LAN:

- caratteristiche di una rete locale Wireless
- le frequenze utilizzate.

Lo standard HyperLAN e sue evoluzioni.

Lo standard 802.11 e sue evoluzioni.

L'interfaccia radio Wi-Fi: tecniche trasmissive:

- modulazioni multiportante: OFDM
- tecniche MIMO.

Il livello 2 del Wi-Fi: gestione del canale radio.

Caratteristiche e configurazione degli apparati.

Problematiche di copertura wireless indoor e outdoor.

Progettazione di una rete Wi-Fi.

La gestione della QoS.

Aspetti commerciali: le molteplici applicazioni del Wi-Fi:

- home networking; reti corporate; accesso pubblico (hot spot).

Aspetti normativi:

- utilizzo in ambito privato e pubblico
- copertura su suolo pubblico.

La mobilità nel Wi-Fi:

- handover e roaming
- mobilità di livello IP.

Il problema della sicurezza dell'accesso e della riservatezza dei dati:

- accesso tramite SSID
- MAC Filtering
- integrità e riservatezza attraverso WEP
- 802.1x (EAP-TLS)
- WPA e WPA2
- WPS
- autenticazione tramite Radius o Captive Portal.

Obiettivi

Illustrare le caratteristiche tecniche del Wi-Fi. Alla fine del corso i partecipanti hanno le competenze per configurare gli apparati di una WLAN e per progettare una copertura radio.

Destinatari

Personale tecnico e non tecnico di operatori di TLC e aziende manifatturiere, specialisti ICT.

Prerequisiti

Conoscenze di base sulle reti per dati, sui protocolli Ethernet e IP.



Long Term Evolution (LTE)

La continua evoluzione delle tecnologie per la mobilità ha prodotto tecniche trasmissive sulla interfaccia radio molto sofisticate, una architettura di core network che deve supportare le prestazioni e la complessità delle applicazioni multimediali consentite dall'elevata velocità di trasmissione della rete d'accesso.
Il corso illustra le importanti novità tecniche della tecnologia radio LTE (Long Term Evolution) e le evoluzioni architetturali della rete rispetto ai sistemi 3G.

Agenda (2 giorni)

Richiami agli aspetti principali della trasmissione radio.

Introduzione a LTE.

OFDM (Orthogonally Frequency Division Multiplexing).

Tecniche di accesso multiplo:

- OFDMA in downlink
- SC-FDMA in uplink.

Codifica e modulazione adattativa.

Tecniche di trasmissione MIMO (Multiple Input Multiple Output).

Il livello fisico:

- Downlink
- Uplink.

I canali:

- canali logici
- canali di trasporto
- canali fisici.

Architettura protocollare:

- User plane
- Control plane.

Architettura di rete.

E-RAN.

Serving Gateway.

Mobility Management Entity.

Packet Data Network Gateway.

Mobility management.

Prestazioni.

Considerazioni implementative.

Aspetti di servizio.

Obiettivi

Illustrare i principali aspetti della tecnologia radio.

Destinatari

Ingegneri e tecnici di rete di operatori di TLC, personale tecnico di aziende manifatturiere di apparati di TLC, personale tecnico di Service Providers, specialisti ICT.

Prerequisiti

Conoscenze dei sistemi radiomobili cellulari. Conoscenze di base della trasmissione radio e dei protocolli TCP/IP.



Long Term Evolution (LTE): Radio Access Network

Il corso mira ad approfondire il funzionamento della tecnologia LTE nella parte di rete di accesso radio. Vengono illustrate le novità sulle tecniche trasmissive utilizzate nel 4G sulla parte radio, per poi descrivere le procedure di gestione dei canali radio e della mobilità. Verranno poi fatte considerazioni in merito agli aspetti implementativi e alle prestazioni reali raggiungibili.

Agenda (3 giorni)

Richiami agli aspetti principali della trasmissione radio:

- la propagazione radio
- il canale radiomobile: attenuazione, multipath, fading, interferenza cocanale
- modulazioni numeriche
- modulazioni ad alta efficienza spettrale.

Introduzione a LTE:

- perché LTE
- i limiti del 3G e dell'HSPA
- evoluzione dei servizi dati su mobile.

Evoluzione degli standard 3GPP: dalla Rel 5 alla Rel. 10.

OFDM (Orthogonally Frequency Division Multiplexing).

Tecniche di accesso multiplo:

- OFDMA in downlink
- SC-FDMA in uplink.

Codifica e modulazione adattativa.

Tecniche di trasmissione MIMO (Multiple Input Multiple Output):

- Diversity
- Beamforming
- SDM
- prestazioni del MIMO.

Channel aggregation.

Le frequenze di funzionamento di LTE:

- le frequenze LTE in Italia
- considerazioni implementative e impatto sulla copertura
- riuso di frequenza e tecniche di pianificazione cellulare.

Copertura radio e pianificazione cellulare.

Il livello fisico:

- Downlink
- Uplink.
- CQI/PMI/RI Reporting
- AMC.

I canali:

- canali logici
- canali di trasporto e canali fisici
- canali downlink
- canali uplink.

Architettura protocollare:

- User plane
- Control plane.

Architettura di rete.

E-RAN.

Long Term Evolution (LTE): Radio Access Network

EPC:

- Serving Gateway
- Mobility Management Entity
- Packet Data Network Gateway

Le interfacce LTE.

Architetture protocollari delle varie interfacce.

Il livello MAC.

DRX, RLC, TM / UM / AM Modes, PDCP,RRC, HARQ, Power Control.

Admission Control e Congestion Control.

Scheduling: Downlink e Uplink.

Mobility management:

- Tracking area
- Cell Selection
- Cell Camped Procedures
- Intra-frequency Reselection
- Inter-frequency Reselection
- Inter-RAT Reselection.

Handover: tipologie di handover in LTE.

La gestione della QoS.

Interoperabilità LTE con altre reti (3G, WiFi, ADSL, ...).

Voice over LTE:

- VoLTE
- CS Fall Back
- VoLGA.

Prestazioni:

- Bit rate massimi
- considerazioni sul throughput reale in diverse condizioni.

LTE Advanced.

Evoluzione della sicurezza in LTE.

Obiettivi

Illustrare gli aspetti della tecnologia LTE nella parte di rete radio.

Destinatari

Ingegneri e tecnici di rete di operatori di TLC, personale tecnico di aziende manifatturiere di apparati di TLC, personale tecnico di Service Providers, specialisti ICT.

Prerequisiti

Conoscenze di base sulla trasmissione numerica, sulla trasmissione radio e sulle reti radiomobili fino al 3G.



Long Term Evolution (LTE): aspetti avanzati

Il corso mira ad approfondire il funzionamento della tecnologia LTE, sia nella parte di rete radio che in quella di core network. Particolare attenzione è rivolta agli aspetti di servizio e alla interazione della rete LTE con elementi esterni, quali ad es. le piattaforme di controllo tipo IMS, per l'implementazione di servizi avanzati. Sono poi fatte considerazioni in merito agli aspetti implementativi e alle prestazioni reali raggiungibili.

Agenda (5 giorni)

Richiami agli aspetti principali della trasmissione radio:

- la propagazione radio
- il canale radiomobile: attenuazione, multipath, fading, interferenza cocanale
- modulazioni numeriche
- modulazioni ad alta efficienza spettrale.

Introduzione a LTE:

- perché LTE
- i limiti del 3G e dell'HSPA
- evoluzione dei servizi dati su mobile.

Evoluzione degli standard 3GPP:dalla Rel 5 alla Rel. 10.

OFDM (Orthogonally Frequency Division Multiplexing).

Tecniche di accesso multiplo:

- OFDMA in downlink
- SC-FDMA in uplink.

Codifica e modulazione adattativa.

Tecniche di trasmissione MIMO (Multiple Input Multiple Output).

- Diversity
- Beamforming
- SDM
- prestazioni del MIMO.

Channel aggregation.

Le frequenze di funzionamento di LTE:

- le frequenze LTE in Italia
- considerazioni implementative e impatto sulla copertura
- riuso di frequenza e tecniche di pianificazione cellulare.

Architettura protocollare:

- User plane e Control plane.

Architettura di rete.

E-RAN.

EPC:

- Serving Gateway.
- Mobility Management Entity.
- Packet Data Network Gateway.

Le interfacce LTE.

Architetture protocollari delle varie interfacce.

Il livello fisico:

- Downlink
- Uplink.
- CQI/PMI/RI Reporting
- AMC.

Il livello MAC.

Long Term Evolution (LTE): aspetti avanzati

DRX, RLC, TM / UM / AM Modes, PDCP,RRC, HARQ, Power Control.

I canali:

- canali logici
- canali di trasporto
- canali fisici.
- canali downlink e canali uplink.

Admission Control e Congestion Control.

Scheduling: Downlink e Uplink.

Mobility management:

- Tracking area
- Cell Selection e Cell Camped Procedures
- Intra-frequency Reselection; Inter-frequency Reselection
- Inter-RAT Reselection.

Handover: tipologie di handover in LTE.

La gestione della QoS:

- EPS bearer: significato e diverse tipologie
- classi di servizio sulla RAN
- QoS in EPC.

Interoperabilità LTE con altre reti (3G, WiFi, ADSL, ...).

Voice over LTE: VoLTE; CS Fall Back; VoLGA.

Cenni a IMS e interazione con la rete LTE.

Prestazioni: Bit rate massimi; considerazioni sul throughput reale in diverse condizioni.

Considerazioni implementative.

La costruzione della RAN:

- implementazione del SGW: alternative tecnologiche e architetturali
- implementazione del PDN GW: alternative tecnologiche e architetturali.

Il backhauling degli e-NB: alternative tecnologiche e architetturali.

Tipologie e classi di terminali LTE.

Aspetti di servizio.

Evoluzione della sicurezza in LTE.

Cenni al protocollo Diameter e utilizzo in LTE.

Roaming LTE:

- scenari di roaming: in e out
- Roaming dati tradizionale e local breakout
- GRX e IPX.

Traffic offload.

LTE Advanced.

Obiettivi

Illustrare gli aspetti della tecnologia LTE sia nella parte di rete radio che in quella di core network.

Destinatari

Ingegneri e tecnici di rete di operatori di TLC, personale tecnico di aziende manifatturiere di apparati di TLC, personale tecnico di Service Providers, specialisti ICT.

Prerequisiti

Conoscenze di base sulla trasmissione numerica, sulla trasmissione radio e sulle reti radiomobili fino al 3G.



Evoluzione della Core Network Mobile dal GSM al 4G

Il corso descrive la evoluzione della Core Network delle reti radiomobili a partire dalle tecnologie 2G con particolare approfondimento su LTE. Viene illustrata l'architettura "all IP" della EPC (Evolved Packet Core), sia nella parte funzionale che implementativa, e la interazione con altri elementi della rete per la fornitura dei vari servizi dalla fonia al multimedia. Infine si darà una visione sulle nuove implementazioni basate sulle tecniche di virtualizzazione.

Agenda (3 giorni)

La core Network delle reti 2G:

- la parte CS Circuit Switched
- la parte PS Packet Switched.

Architettura della rete UMTS.

Differenze e analogie tra rete mobile 2G e rete mobile 3G:

- funzioni principali della rete core UMTS
- protocolli utilizzati nella rete mobile 3G: evoluzione della segnalazione SS7
- rel 99: La doppia Core Network
- rel 4: Introduzione del concetto di MSC-Server e Media Gateway, e switching su backbone non-TDM (ATM, IP)
- rel 5: Evoluzione della rete GPRS in rete Packet Switching 3G
- evoluzione degli standard 3GPP:dalla Rel 5 alla Rel. 10.

Architettura della rete LTE.

Evoluzione della rete verso All IP: la rete SAE/EPC, Evolved Packet System (EPS):

- la rete mobile LTE come rete universale di telecomunicazioni dati e servizi multimediali
- interfaccia tra rete di accesso radio e rete core
- gestione dei bearer radio e QoS
- evoluzione dei criteri di sicurezza 3G in LTE.

Funzioni principali della rete core SAE/EPC:

- elementi della rete EPC: MME, S-GW, PDN-GW
- le interfacce LTE
- architetture protocollari delle varie interfacce
- gestione della mobilità, della segnalazione di controllo e del traffico utente
- evoluzione del HLR in HSS: nuove funzioni e gestione della sicurezza
- nuovi protocolli di rete basati su IP: protocollo Diameter, evoluzione GTP v2
- interlavoro con la rete pre-4G per gestione del traffico voce prima della introduzione di VoLTE: CS Fallback (CSFB)
- interlavoro della rete LTE con altre tecnologie non 3GPP.

IP Multimedia SubSystem (IMS):

- introduzione del concetto IMS e sua evoluzione
- architettura della rete con l'introduzione degli elementi di IMS
- principali procedure di rete legate a IMS: protocollo SIP, autenticazione e registrazione
- gestione delle connessioni nella rete IMS.

Voice over LTE (VoLTE):

- definizione del servizio VoLTE
- principali caratteristiche del servizio VoLTE
- procedure IMS inerenti VoLTE
- gestione delle chiamate VoLTE nella rete 4G
- interlavoro per voce tra rete 4G e reti pre-4G: compatibilità tra VoLTE e telefonia tradizionale
- impatti nella rete 2G/3G per interlavoro con VoLTE (SRVCC)
- nuovi aspetti di roaming con l'introduzione di IMS e VoLTE.

Le nuove soluzioni virtualizzate della EPC.

Evoluzione della Core Network Mobile dal GSM al 4G

Obiettivi

Illustrare in dettaglio gli elementi e il funzionamento della Core Network LTE.

Destinatari

Ingegneri e tecnici di rete di operatori di TLC, personale tecnico di aziende manifatturiere di apparati di TLC, personale tecnico di Service Providers, specialisti ICT.

Prerequisiti

Conoscenze di base sulle reti radiomobili e sulle architetture protocollari TCP/IP.

Pricing



Mai più senza il corso!

ISCRIZIONE GOLD

scopri i vantaggi che offre questa formula

- ✓ con l'*iscrizione Gold* se il corso che ti interessa non è in calendario potrai *concordare con noi la data* e lo inseriremo al più presto nella programmazione

- ✓ la formula assicura che *l'edizione* è *garantita*

Come può un'Azienda perfezionare una iscrizione Gold?

Si attiva con l'*iscrizione* di almeno *due partecipanti* della stessa azienda inviando per fax il modulo di iscrizione compilato in tutte le sue parti e la copia del bonifico.

E se un'Azienda ha un singolo partecipante?

È possibile perfezionare un'*iscrizione Gold*, anche in presenza di un *solo partecipante*. In questo caso alla quota di iscrizione va aggiunta l'*Opzione Gold* (pari al 90% della quota d'iscrizione). Poiché il corso è a catalogo, ulteriori iscrizioni potranno giungere da altre aziende; in tal caso l'Opzione Gold sarà *rimborsata*.

Con l'iscrizione Gold il corso si terrà anche se rimarrai l'unico iscritto!

Partecipazioni Multiple ad uno stesso corso

Per i corsi a catalogo, sono previsti *sconti* per le partecipazioni multiple che provengono da una stessa Azienda:

- *10%* sulla *seconda* partecipazione
- *40%* sulla *terza*
- *80%* dalla *quarta* partecipazione in poi.

Lo sconto è attivo solo inviando scheda di iscrizione e copia dell'avvenuto pagamento prima dell'edizione del corso.

Di seguito sono riportati tutti i corsi a catalogo, con l'indicazione della sigla, titolo, durata e Quota di iscrizione.
La ***Quota di iscrizione*** comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Gli sconti per le ***iscrizioni multiple sono riportati nella sezione precedente***.

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
	Benessere Organizzativo e Gestione dello Stress (BEO)		
BEO832	Tecniche di Gestione dello Stress	2	1.090
BEO833	Viva il Lunedì	2	1.090
BEO834	La resilienza: una risorsa per il benessere	2	1.090
BEO836	Tutelare la salute psicofisica e promuovere il benessere individuale e collettivo nei luoghi di lavoro	1	590
BEO838	Lo stress lavoro correlato: il decreto legislativo, il significato e il modello di intervento	1	590
	Strumenti di Direzione Aziendale (DAZ)		
DAZ730	Finanza per non specialisti	3	1.440
DAZ735	Budget e Controllo di Gestione per non specialisti	3	1.440
DAZ738	Economics per il successo dell'impresa	3	1.540
DAZ741	Business Planning: pianificazione strategica e economico finanziaria	3	1.540
	Basi Dati e Servizi(DBS)		
DBS550	Basi di dati relazionali: metodologie di progetto e di analisi dei dati	2	1.090
DBS551	Il linguaggio SQL per utenti	2	1.640
DBS552	Il linguaggio SQL: Base	3	1.540
DBS553	Il linguaggio SQL: Avanzato	2	1.280
DBS554	Database in ambiente Oracle: PL/SQL	3	1.640
DBS560	Introduzione alla Business Intelligence	2	1.190
DBS561	Strumenti per la Business Intelligence	2	1.190
DBS564	Data Mining	3	1.640
DBS565	Data Mining per il supporto alle decisioni aziendali	2	1.190
DBS570	Data Warehouse: analisi dei dati a supporto delle decisioni aziendali	5	2.480
DBS572	Sviluppo di procedure ETL in Datastage	4	1.980
	La Gestione del Cambiamento (GEC)		
GEC952	Gestione della complessità	3	1.640
GEC954	Il governo del cambiamento	2	2.240
GEC956	Il pensiero flessibile	3	1.540
GEC958	Problem solving e decision making in situazioni di crisi	3	1.540

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
La Gestione delle Relazioni (GRE)			
GRE932	Negoziazione e gestione dei conflitti	5	2.240
GRE934	Team building e teamwork	3	1.540
GRE935	Consulting Skill for IT Professionals	2	1.090
GRE936	La costruzione della squadra	3	1.540
GRE937	La comunicazione efficace con il modello del process communication®	2	1.090
GRE938	La gestione delle riunioni	2	1.090
GRE939	Gestire il proprio ruolo nell'interfunzionalità	3	1.540
Sistemi Gestionali (GST)			
GST782	La Gestione delle persone e delle competenze	4	1.790
GST784	Il colloquio di valutazione e di feedback	3	1.540
GST786	L'intervista di selezione	2	1.090
GST787	Assessment e Development Center	3	1.540
GST790	Il processo di Formazione	4	1.790
GST791	Formazione Formatori	3	1.540
Reti IP (IPN)			
IPN210	Ethernet: dalle reti locali alle reti metropolitane	3	1.540
IPN214	Le Reti Metro Carrier Ethernet	2	1.280
IPN218	Introduzione alle reti per dati ed al Cisco IOS	5	2.060
IPN220	Internet e il protocollo IP per non tecnici	2	1.090
IPN221	Fondamenti di Internet, IPv4 ed IPv6	5	2.060
IPN222	Networking IP in ambiente Cisco	5	2.060
IPN232	Routing IP nell'IOS Cisco	5	2.400
IPN233	Routing IP nell'IOS XR Cisco	3	1.790
IPN234	Troubleshooting di reti Cisco	5	2.400
IPN236	Cisco Nexus 7000 Switch per Data Center	3	2.290
IPN238	Configurazione, esercizio e manutenzione dei router Cisco Hi-End con sistema operativo IOS-XR	3	1.980
IPN242	Strumenti Open Source per il Network Management	3	1.540
IPN246	BGP: aspetti base	3	1.540
IPN247	BGP: aspetti avanzati	3	1.640
IPN249	Routing Multicast	3	1.640
IPN252	Introduzione alla Configurazione di Router Juniper	3	1.280
IPN253	Routing IP nel JUNOS Juniper: aspetti di base	3	1.540
IPN254	Routing IP nel JUNOS Juniper: aspetti avanzati	4	2.400
IPN255	Routing multicast nel JUNOS Juniper	2	1.280
IPN256	Carrier Ethernet in ambiente Juniper	2	1.280
IPN257	Switching nel JUNOS Juniper	3	1.640
IPN258	MPLS nel JUNOS Juniper	5	3.100

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
IPN259	QoS IP nel JUNOS Juniper	2	1.280
IPN260	Aspetti avanzati del Routing IP nelle reti Enterprise Juniper	3	1.980
IPN261	Aspetti avanzati delle Reti Switched Ethernet Juniper	2	1.640
IPN262	Multilayer Switching e Reti di Campus	5	2.400
IPN264	Il Routing IP nelle Reti ISP: aspetti di base	5	2.700
IPN265	Il Routing IP nelle Reti ISP: aspetti avanzati	5	2.840
IPN266	Tecnologie dei backbone nelle reti ISP	5	2.840
IPN267	Servizi VPN nelle reti ISP	5	2.840
IPN269	Next Generation Multicast VPN	2	1.280
IPN272	MPLS: dalla Teoria alla Pratica	3	1.540
IPN273	MPLS: servizi avanzati	3	1.640
IPN276	MPLS nell'IOS XR Cisco	3	1.980
IPN650	Networking IP in ambiente Huawei	8	2.480
IPN652	Networking IP in ambiente Huawei - Fast Track	4	1.790
IPN654	Enterprise Routing in tecnologia Huawei	5	1.880
IPN655	Enterprise Switching in tecnologia Huawei	5	1.880
IPN656	Sicurezza, Alta Affidabilità e QoS in Tecnologia Huawei	5	1.930
IPN660	Soluzioni di Wan Governance: IPANEMA	2	1.280
IPN670	IPV6 e gli scenari di migrazione	1	640
IPN672	IPv6: istruzioni per l'uso	4	1.980
IPN674	IPv6 nelle reti ISP	3	1.640
IPN675	Routing IPv6 nell'IOS XR Cisco	3	1.980
IPN676	IPv6 nel JUNOS Juniper	3	1.640
IPN680	Evoluzione delle reti IP Broadband: fondamenti e linee guida	3	1.790
IPN682	Software Defined Networking (SDN), OpenFlow e Network Function Virtualization (NFV)	2	1.190
IPN684	Cloud Computing Networking	2	1.190
	Servizi IP (IPS)		
IPS282	La Qualità del Servizio nelle reti IP	2	1.190
IPS284	Cisco Voice over IP	4	1.790
IPS286	Voice over IP: architetture, protocolli e servizi	4	1.790
IPS288	IP-TV. La TV digitale sulle nuove reti dati	2	1.090
IPS292	Segnalazione su IP: SIP e DIAMETER	3	1.640
IPS294	SIP: architetture, protocollo e servizi	3	1.640
IPS296	IMS: architettura e applicazioni in ottica NGN	3	1.640
IPS681	Avaya Aura Communication Manager: Design, Configurazione e Troubleshooting	3	1.790
IPS685	Asterix	4	2.190
IPS690	CCNA Voice	5	2.400
IPS691	Voice Communications and QoS in ambiente Cisco	5	2.480

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
IPS692	Cisco Unified Communications Manager: Base	5	2.480
IPS693	Cisco Unified Communications Manager: Avanzato	5	2.480
IPS694	Troubleshooting Unified Communications in ambiente Cisco	5	2.480
IPS695	Cisco Unified Communications Applications	5	2.480
	Servizi IT (ITS)		
ITS483	ITIL® v3: Overview per Manager	1	690
ITS484	ITIL® v3 Foundation	3	1.090
ITS485	ITIL® V3 Intermediate	3	1.280
ITS486	ITIL® V3 Managing Across Lifecycle	3	1.280
ITS490	COBIT® 5	2	1.090
ITS494	Cloud Computing	3	1.640
ITS495	Data Center: Storage Networking e Server Virtualization	3	1.790
ITS496	Nuove Architetture per Data Centre nell'approccio Cisco Systems	2	1.280
ITS497	Progettazione e configurazione di soluzioni Cisco Unified Computing	3	1.640
ITS498	Virtualizzare con VMware: Progetto e Implementazioni	3	1.790
	Linguaggi ed Architetture software (LAP)		
LAP391	Excel Avanzato: importazione, analisi e reporting	3	1.190
LAP394	Excel VBA	2	940
LAP504	Programming in C#	5	1.640
LAP507	Strumenti per il WEB: Applicazioni ASP	3	1.440
LAP508	Developing ASP.NET MVC 4 Web Applications	5	1.640
LAP509	Strumenti per il WEB: Creare animazioni con Adobe Flash CS5.5	3	1.440
LAP510	XML e tecnologie afferenti	3	1.540
LAP512	La programmazione Object Oriented in Java	4	1.640
LAP513	Web programming e usabilità con PHP e MySQL	3	1.440
LAP515	Gang of Four Design Patterns	3	1.540
LAP516	Lo sviluppo di applicazioni di business con gli Enterprise Java Bean 3.1	4	1.980
LAP518	Sharepoint 2010 Business Intelligence	4	1.790
LAP520	Il Framework Struts	3	1.540
LAP521	Il Framework Hibernate	3	1.640
LAP522	Sviluppo di applicazioni Web con Servlet e JSP	4	1.790
LAP523	Cloud Computing: porting e progettazione di applicazioni e servizi	3	1.540
LAP524	JBOSS for Administrators	4	1.980
LAP525	Linux, Apache, MySQL, PHP (LAMP)	3	1.540
LAP526	CMS JOOMLA - Base	3	1.090
LAP527	Pubblicazione di contenuti su Web con piattaforme open source	3	1.540
LAP528	Progettazione Object Oriented con UML	3	1.540
LAP530	Progettazione e Governance di architetture SOA	3	1.540

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
LAP531	XML e SOA	3	1.440
LAP532	Service-Oriented Architecture (SOA): orchestrazione e integrazione di servizi di business	3	1.540
LAP534	Evoluzione delle applicazioni per l'e-business dalle web application verso la Service-Oriented Architecture (SOA)	3	1.640
LAP536	Sviluppo di applicazioni con il framework Spring	3	1.640
LAP540	System Integration: scenari, tecnologie e metodologie	2	1.280
LAP542	NG-OSS (Next Generation Operational Support System)	2	1.280
LAP543	Usabilità ed accessibilità dei Siti Web e lo standard W3C	2	1.190
LAP544	Usabilità: progettazione dei servizi e delle applicazioni	3	1.540
LAP545	Le piattaforme applicative per dispositivi mobili	3	1.540
LAP546	Objective C per iOS	4	1.790
LAP547	Android: progettazione di applicazioni per terminali mobili	5	2.240
	Lo Sviluppo della Leadership (LDR)		
LDR980	Laboratorio per lo sviluppo della leadership	2	2.240
LDR982	Leadership e Coaching	3	1.540
LDR984	Gestire le Risorse Umane: aree e strumenti di intervento	4	1.790
LDR986	La sfida della fiducia: dall’efficacia all’eccellenza	2	1.090
LDR988	Lean Leadership	2	2.240
	Aspetti Legali, Normativi e di Regolamentazione (LEG)		
LEG850	La privacy: aspetti tecnici, organizzativi e legali per le aziende	3	1.540
LEG851	Il nuovo Regolamento Europeo sulla Protezione dei dati personali	2	1.280
LEG853	Security Manager: Sicurezza e protezione delle informazioni Personali e Istituzionali	2	1.280
LEG854	Data Privacy e Data Protection nelle Infrastrutture Critiche nazionali	3	1.540
LEG855	Security vs Privacy: misure per la protezione e conservazione dei dati di traffico telefonico e telematico	3	1.540
LEG857	La responsabilità amministrativa e penale delle Persone Giuridiche (ex D. Lgs. 231/2001)	1	690
LEG860	Gli appalti per la fornitura di beni e di servizi informatici e telematici nella Pubblica Amministrazione	4	1.790
LEG864	La Conservazione Sostitutiva a norma, Fatturazione Elettronica e Privacy	3	1.640
LEG870	Frode di Identità e Falso Documentale: tecniche e conoscenze per verificare i documenti di identità	1	690
LEG872	La proprietà intellettuale in rete	3	1.540
LEG874	Profili Giuridici dei contratti tra imprese: come costituire, redigere ed interpretare un contratto commerciale	3	1.540
LEG876	Profili giuridici del Commercio Elettronico	3	1.540
LEG880	La regolamentazione dei servizi di TLC	1	1.190
LEG881	Gli aspetti giuridici nella regolamentazione del mercato di TLC	1	1.190
LEG891	La gestione economico-giuridica dell'innovazione	2	1.090
LEG893	Diritti di proprietà Industriale : il Brevetto	1	640
LEG894	Diritti di proprietà Industriale : il Marchio	1	640

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
	Marketing & Sales (MKS)		
MKS750	Il successo nella vendita	3	1.540
MKS752	Strategie e tecniche di vendita per il mercato Business	3	1.540
MKS755	Gestire con successo la forza vendita	3	1.540
MKS758	Le Vendite Complesse	3	1.790
MKS760	Vendere in un Mercato in Flessione	2	1.280
MKS762	In sintonia con il cliente per vendere servizi informatici e telematici	3	1.540
MKS764	Vendere soluzioni ICT	3	1.640
	Strategic Management (MNG)		
MNG700	Strategic Management: Corporate & Business Strategies	3	1.540
MNG705	Compliance & Risk Management	2	1.090
MNG707	Governance, Corporate Risk management & Compliance	3	1.640
MNG710	Performance Management: valutazione e gestione delle performance	3	1.540
MNG711	Migliorare i risultati aziendali con la leva dei processi	2	1.640
MNG712	Strumenti e metodologie di Business Process Management	3	1.540
MNG715	L'approccio Agile all'Informatica a supporto del BPM e Lean & Digitize	3	1.540
MNG716	Design Thinking for Process Improvement	2	1.090
MNG717	Change Management: la gestione efficace dei cambiamenti organizzativi	2	1.190
MNG718	Change & Innovation	1	590
MNG719	Business Excellence Models: percorsi verso l'eccellenza	3	1.540
MNG725	International Business Management	3	1.640
	Reti e Servizi di TLC (NET)		
NET020	Le Telecomunicazioni "senza formule"	5	2.060
NET022	Reti di telecomunicazione: servizi, architetture e protocolli	5	2.060
NET024	I cablaggi strutturati negli edifici e nei Data Center: progettazione e normative	3	1.640
NET028	Evoluzione delle reti per fonia	3	1.540
NET034	Evoluzione dei Servizi e delle Reti di TLC	2	1.190
NET038	NGN (Next Generation Networks): le reti di TLC di nuova generazione	2	1.190
NET042	Televisione digitale e standard DVB	3	1.540
NET044	Sistemi di trasmissione radio via satellite	5	2.480
NET045	Reti Satellitari: aspetti applicativi	2	1.190
NET046	Reti Satellitari: Tecnologie, architetture e servizi	3	1.790
NET048	Ottimizzazione delle codifiche e compressione sui Carrier satellitari	5	1.480
NET050	Fondamenti della trasmissione numerica: il segnale dall'origine al transito su una fibra ottica	3	1.440
NET055	Evoluzione delle reti di trasporto trasmissive: dalla SDH alla PTN	3	1.540
NET060	Sistemi di alimentazione, di emergenza e fiscalità energetica	3	1.790
NET062	Qualità dei sistemi e dei servizi nelle reti di telecomunicazioni: parametri e misure	3	1.640
NET064	Monitoraggio del traffico di Rete	3	1.640

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
NET065	ADSL e Sistemi DSL per non tecnici	2	1.090
NET066	ADSL e Sistemi DSL: tecnologie e applicazioni	3	1.540
NET069	Sistemi DSL e Reti a larga banda	3	1.540
NET070	Diagnosi e localizzazione dei guasti nei cavi per TLC in rame	2	1.190
NET071	Misure per la caratterizzazione della linea per sistemi xDSL	2	1.190
NET073	Sviluppo della rete di accesso in fibra ottica NGAN (Next Generation Access Network)	5	2.480
NET074	NGAN - Next Generation Access Network	3	1.790
	Sistemi Operativi (OPS)		
OPS602	Architettura UNIX ed ambiente utente	5	2.060
OPS604	La gestione di un server UNIX su una rete IP	5	2.240
OPS610	Linux System & Network Administration	5	2.480
OPS620	Microsoft Windows 8	5	1.640
OPS622	Microsoft Windows 2012	5	1.640
OPS624	Windows 8/2012: amministrazione remota e scripting	3	1.540
OPS630	Windows/Unix:interoperabilità dei servizi di rete	3	1.540
	Project Management (PRJ)		
PRJ803	One Page Project Map	2	1.280
PRJ805	Basics di Project management	3	1.440
PRJ807	Microsoft Project - Base	2	1.040
PRJ808	Microsoft Project - Avanzato	2	1.090
PRJ810	Lavorare per progetti	5	2.240
PRJ812	La gestione dei progetti ICT	5	2.240
PRJ816	Project Management Professional : Certificazione PMP/PMI®	8	4.500
PRJ818	La gestione dei rischi e delle opportunità di progetto	3	1.540
PRJ820	Le capacità manageriali del project manager	3	1.540
PRJ821	IT Planning & Programming	2	1.090
PRJ824	Agile Project Management	2	1.190
	Scenari e contesti (SCN)		
SCN400	Il settore ICT&M nel contesto economico e di mercato	2	1.090
SCN404	Scenari di mercato delle telecomunicazioni	2	1.190
SCN408	Il Mobile Marketing	1	590
SCN410	Web 2.0 & Social Networking: scenari e impatti	1	640
SCN412	Enterprise 2.0: applicazioni, modelli e scenari di mercato	1	640
SCN414	Cloud Oriented	1	640
SCN418	On-line Marketing: le nuove modalità del marketing in rete	2	1.090
SCN420	CRM in azienda: approcci, applicazioni e scenari	1	590
SCN424	SEM: Search Engine Marketing. Come ottenere visibilità in rete	1	590
SCN428	Il Podcasting aziendale: modelli, opportunità e scenari evolutivi	1	590
SCN430	Open Innovation e Crowdsourcing: modelli, esperienze, opportunità e criticità	1	590

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
SCN432	Gli Advergames: opportunità, criticità e prospettive di sviluppo	1	590
SCN434	Innovation Driving Design Thinking	2	1.190
SCN435	Pubblica Amministrazione e sviluppo della Banda Larga e Ultralarga	1	640
SCN436	Innovazione nella PA: dal CAD all'Agenda Digitale	2	1.090
SCN438	La Conservazione Sostitutiva	2	1.280
SCN440	La gestione documentale	3	1.640
Sicurezza delle Reti e delle Applicazioni (SEC)			
SEC302	La sicurezza dei sistemi, dei dati e delle reti	5	2.240
SEC303	Cyber Security: Minacce e Criteri di Protezione	3	1.790
SEC304	Tecniche di attacco di un sistema informatico	3	1.790
SEC305	Tecniche di difesa di un sistema informatico	3	1.790
SEC306	Ethical Hacking e Penetration Test di Applicativi Web	3	2.060
SEC307	Ethical Hacking e Penetration Test: dalla teoria alla pratica	5	3.490
SEC308	Sicurezza di rete: firewall, IPS e VPN	4	1.790
SEC309	OpenVPN e CISCO VPN	4	2.190
SEC314	Reti sicure in ambiente SonicWall: aspetti di base	2	1.190
SEC316	Reti sicure in ambiente Cisco, difesa perimetrale con IOS Firewall	5	2.400
SEC318	PCI DSS v2.0 (Payment Card Industry Data Security Standard)	2	1.280
SEC320	Reti sicure in ambiente Cisco, difesa perimetrale e accesso remoto con ASA NG	5	2.400
SEC323	La sicurezza nei Sistemi operativi Windows: aspetti e strumenti di gestione	5	2.240
SEC324	Progettare e realizzare la sicurezza di Sistemi Operativi Microsoft Windows	5	2.240
SEC325	La sicurezza nei Sistemi operativi UNIX/Linux	4	1.980
SEC326	Application Security: criteri e aspetti operativi per lo sviluppo di applicazioni sicure	3	1.640
SEC328	Autorità di certificazione, certificati digitali, carta nazionale dei servizi e posta elettronica certificata	3	1.640
SEC330	Rilevamento della sicurezza di un sistema informatico	3	1.640
SEC331	ICT Security: aspetti di base	3	1.540
SEC332	Gestione degli incidenti in un sistema informativo (Incident Management)	3	1.640
SEC333	La gestione della Continuità Operativa - Business Continuity Management	3	1.790
SEC334	Analisi dei Rischi Informatici	3	1.540
SEC335	La gestione della Sicurezza dell'Informazione (ISMS): la norma ISO IS 27001	3	1.640
SEC337	Aggiornarsi alla norma ISO/IEC 27001:2013 e tematiche di Audit	2	1.280
SEC338	Informatica Forense (Computer Forensics): aspetti pratici	3	1.790
SEC339	Digital Forensics	3	1.790
SEC340	Analisi Forense dei Dispositivi Mobili (Mobile Forensics)	3	1.640
SEC342	I sistemi di monitoraggio e controllo in rete	3	1.640
SEC344	La Security dei sistemi di IP-Surveillance	2	1.090
SEC350	La Cloud Security	2	1.280
SEC353	Realizzare reti sicure con CheckPoint	3	1.690

Sigla	Titolo	Durata (giorni)	Quota Iscrizione (al netto IVA)
SEC354	Realizzare reti sicure con CheckPoint: aspetti avanzati	4	1.790
SEC357	Reti sicure in ambiente Fortinet: aspetti di base	2	1.190
SEC358	Reti sicure in ambiente Fortinet: aspetti avanzati	3	1.640
SEC360	Unified Access Control: la sicurezza degli endpoint in contesti critici	3	1.640
SEC362	Reti sicure in ambiente Juniper: aspetti base	4	2.190
SEC363	Reti sicure in ambiente Juniper: aspetti avanzati	5	3.100
SEC370	CCNA Security	5	2.300
SEC374	Reti sicure in ambiente Cisco, difesa perimetrale con IOS e ASA	5	2.700
SEC375	Reti sicure in ambiente Cisco, difesa perimetrale avanzata con ASA	5	2.700
SEC376	Reti sicure in ambiente Cisco, identificazione ed accessi sicuri	5	2.700
SEC377	Reti sicure in ambiente Cisco, connessioni remote e VPN	5	2.700
	Strumenti per l'Efficacia Personale (SEP)		
SEP900	La comunicazione brillante e efficace	3	1.540
SEP903	Effective Work Habits	2	1.090
SEP912	Smart Memory: apprendimento rapido ed efficace	3	1.540
SEP914	Lettura strategica: massimo rendimento, minimo sforzo	3	1.540
SEP916	Mind Mapping: come ridurre un documento del 90%	3	1.540
SEP920	Public Speaking: l'arte della persuasione	3	1.540
SEP924	Time Management	2	1.090
SEP925	Laboratorio di Gestione del Tempo	2	1.280
SEP926	L'Intelligenza emotiva: una risorsa per l'efficacia personale	2	2.240
	Reti e Servizi Wireless (WIR)		
WIR104	Tecnologie per la mobilità: dal GSM all'UMTS e HSPA fino a LTE	5	2.240
WIR105	I sistemi radiomobili per non tecnici dal GSM a LTE	2	1.540
WIR106	Evoluzione dei sistemi Radiomobili: verso la quarta generazione	1	640
WIR112	UMTS: la terza generazione delle reti mobili ed evoluzioni verso la quarta generazione	4	1.790
WIR119	La segnalazione nelle reti 3G e sue evoluzioni	4	1.980
WIR126	Multi Environment Networks: evoluzione e integrazione delle tecnologie wireless	3	1.540
WIR132	Wi-Fi e Wi-Max	2	1.190
WIR134	Wireless LAN	3	1.640
WIR140	Long Term Evolution (LTE)	2	1.280
WIR142	Long Term Evolution (LTE): Radio Access Network	3	1.790
WIR144	Long Term Evolution (LTE): aspetti avanzati	5	2.700
WIR146	Evoluzione della Core Network Mobile dal GSM al 4G	3	1.790



Modulo di iscrizione
ai Corsi

Fax +39 0862 028308
mail corsi@ssgrr.com
www.reissromoli.com

Il modulo deve essere compilato nelle due pagine in ogni sua parte ed inviato, allegando copia del pagamento della quota d'iscrizione, via fax al n. *+39 0862 028308*

Partecipanti al corso (sigla)________________ **del** ________________ **sede** ________________

Nome e Cognome	Ruolo	email

Iscrizione GOLD ☐ **Opzione GOLD** (+90% della quota di iscrizione)



Quota di Iscrizione	Totale	
	(in caso di esenzione indicare la motivazione) IVA(21%)	

Dati della Azienda/Ente		
Azienda/Ente		
Indirizzo		
Città	**CAP**	**PR**
P.IVA	**C.F.**	

Referente iscrizione ____

email ____________________________ **tel** ______________ **fax** ______________

Modalità di Pagamento: Bonifico Bancario	
Banca dell'Adriatico	
Codice IBAN	IT 48 J 05748 03602 100000009179

La Fattura va intestata a:		
Azienda/Ente		
Indirizzo		
Città	**CAP**	**PR**
P.IVA	**C.F.**	
Esenzione IVA ☐	Motivazione	

La Fattura va Inviata a:		
Cognome	**Nome**	
Indirizzo		
Città	**CAP**	**PR**

Fax +39 0862 028308
mail corsi@ssgrr.com
www.reissromoli.com

Condizioni Generali di Fornitura

OGGETTO
Oggetto delle presenti Condizioni Generali è la fornitura da parte di Reiss Romoli s.r.l. di corsi di formazione, il cui elenco, le date ed i prezzi sono riportati sul sito www.reissromoli.com.

ISCRIZIONI
Le iscrizioni possono pervenire fino a 5 giorni lavorativi prima dell'inizio del corso e saranno accettate secondo l'ordine cronologico di arrivo. L'iscrizione è confermata al ricevimento del corrispettivo da parte di Reiss Romoli.

ISCRIZIONE GOLD e OPZIONE GOLD



Se il corso ha l'icona, perfezionando un'Iscrizione GOLD si può concordare la data se il corso non è programmato e avere certezza dell'edizione.
Si perfeziona l'Iscrizione GOLD o iscrivendo almeno 2 partecipanti della stessa azienda o, in presenza di un solo partecipante, con l'aggiunta dell'Opzione GOLD (pari al 90% della quota d'iscrizione).In caso di iscrizione singola, se ulteriori iscrizioni giungono da altre aziende, l'Opzione GOLD sarà rimborsata.

CORRISPETTIVI
Tutti i prezzi pubblicati da Reiss Romoli si intendono IVA esclusa. L'IVA sarà applicata ai sensi di legge.
Le quote di iscrizione comprendono la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

MODALITÀ DI PAGAMENTO
Il cliente corrisponderà a Reiss Romoli s.r.l. gli importi previsti dal listino in vigore al momento dell'iscrizione al corso di interesse ed in base al numero dei partecipanti. Tutte le variazioni saranno specificate esclusivamente con un'offerta scritta emessa da Reiss Romoli.
Il pagamento dovrà avvenire con Bonifico Bancario anticipato intestato a Reiss Romoli s.r.l. – Banca dell'Adriatico – IBAN: IT 48 J 05748 03602 100000009179. La fattura sarà emessa al termine del corso.

DISDETTA
Il Cliente potrà annullare l'iscrizione ai corsi in ogni momento fino al giorno precedente il loro inizio, mediante comunicazione a Reiss Romoli tramite e-mail a corsi@ssgrr.com, oppure tramite fax al numero 0862 028308. Resta inteso che, qualora tale comunicazione non pervenga a Reiss Romoli srl almeno 6 giorni lavorativi prima della data di inizio del Corso, il Cliente sarà tenuto a corrispondere a Reiss Romoli a titolo di penale il 75% del corrispettivo individuale previsto. Il Cliente sarà, comunque, tenuto al pagamento dell'intero corrispettivo individuale, in caso di mancata disdetta, qualora il partecipante non si presenti al Corso alla data stabilita o interrompa la frequenza al corso stesso per cause non attribuibili a Reiss Romoli.
Gli iscritti possono essere sostituiti da nuovi partecipanti a condizione che il corso non abbia ancora avuto inizio.

ANNULLAMENTO
Reiss Romoli si riserva la possibilità di annullare il corso per qualsiasi causa. In tal caso Reiss Romoli rimborserà le quote già pervenute.

DIRITTO D'AUTORE
I materiali e la documentazione distribuiti durante il corso sono di proprietà di Reiss Romoli o dei propri partner e non possono essere riprodotti o distribuiti a terze parti senza autorizzazione scritta dei proprietari.

DISPOSIZIONI GENERALI
Qualsiasi modifica alle presenti Condizioni Generali dovrà essere effettuata per iscritto. Le Condizioni Generali di fornitura saranno comunque prevalenti rispetto a qualsiasi altro accordo.

FORO COMPETENTE
Per qualsiasi controversia riguardo la validità, l'interpretazione e l'esecuzione delle presenti Condizioni Generali, sarà competente il Foro di L'Aquila.

Ai sensi e per gli effetti degli artt. 1341 e 1342 del Codice Civile, il cliente approva espressamente le Condizioni Generali di fornitura

IL CLIENTE

____
Timbro e FIRMA E DATA

LEGGE SULLA PRIVACY

Ai sensi e per gli effetti del DLgs. 30.6.2003 n. 196, relativo alla tutela del trattamento dei dati personali, il cliente fornisce il consenso al trattamento dei dati forniti per scopi amministrativi e marketing-commerciali. Reiss Romoli s. r. l. si impegna a non comunicare tali dati a terze parti. Il cliente ha il diritto di verificare i dati e di richiederne gratuitamente e in qualunque momento la modifica o la cancellazione tramite email a corsi@ssgrr.com

IL CLIENTE

____
Timbro e FIRMA E DATA